



Technical Specification

MEF 15

Requirements for Management of

Metro Ethernet Phase 1 Network Elements

November 2005

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.

© The Metro Ethernet Forum 2005. All Rights Reserved.

Table of Contents

1. ABSTRACT	1
2. TERMINOLOGY	1
3. SCOPE.....	4
4. COMPLIANCE LEVELS.....	4
5. GENERAL REQUIREMENTS.....	4
5.1 MANAGEMENT INTERFACE REQUIREMENTS.....	4
5.2 TRANSPORT LAYER INTERFACES.....	5
6. CONFIGURATION MANAGEMENT REQUIREMENTS.....	5
6.1 UPDATE NOTIFICATIONS	5
6.2 CONFIGURATION BACKUP AND RECOVERY	6
6.3 NETWORK PROVISIONING AND INSTALLATION.....	6
6.4 SERVICE ACTIVATION	12
6.5 STATUS MANAGEMENT AND CONTROL.....	17
7. FAULT MANAGEMENT REQUIREMENTS.....	17
7.1 ALARM SURVEILLANCE	18
7.2 FAULT LOCALIZATION	20
7.3 TESTING	21
8. PERFORMANCE MANAGEMENT REQUIREMENTS.....	21
8.1 GENERAL PERFORMANCE MONITORING REQUIREMENTS.....	22
8.2 MEF SPECIFIC PERFORMANCE MONITORING REQUIREMENTS	23
9. SECURITY MANAGEMENT REQUIREMENTS.....	25
9.1 NE SECURITY MANAGEMENT REQUIREMENTS	25
10. REFERENCES	28

1. Abstract

This document specifies the network management requirements to be met by Provider Edge Metro Ethernet Network Elements supporting Ethernet Service Phase 1 [MEF10] providing Carrier Class Ethernet Services.

2. Terminology

This section provides terminology and acronym definitions in the following table.

Term	Definition
Alarm Status	Indicates the occurrence of an abnormal condition. Values for alarm status include: critical, major, minor, indeterminate, warning, pending, and cleared
All to One Bundling	A UNI attribute in which all CE-VLAN IDs are associated with a single EVC.
Bandwidth Profile	A characterization of ingress Service Frame arrival times and lengths at a reference point and a specification of the disposition of each Service Frame based on its level of compliance with the Bandwidth Profile..
Broadcast Service Frame	A Service Frame that has a broadcast destination MAC address.
Bundling	A UNI attribute in which more than one CE-VLAN ID is associated with an EVC.
CBS	Committed Burst Size
CE	Customer Edge
CES	Circuit Emulation Service
CE-VLAN CoS	Customer Edge VLAN CoS. The user_priority bits in the IEEE 802.1Q Tag in a Service Frame that is either tagged or priority tagged.
CE-VLAN ID	Customer Edge VLAN ID. The identifier derivable from the content of a Service Frame that allows the Service Frame to be associated with an EVC at the UNI.
CE-VLAN ID Preservation	An EVC attribute in which the CE-VLAN ID of an egress Service Frame is identical in value to the CE-VLAN ID of the corresponding ingress Service Frame.
CE-VLAN ID/EVC Map	An association of CE-VLAN IDs and EVCs at a UNI.
CE-VLAN Tag	Customer Edge VLAN Tag. The IEEE 802.1Q Tag in a tagged Service Frame.
CF	Coupling Flag.
Coupling Flag	CF is a Bandwidth Profile parameter. The Coupling Flag allows the choice between two modes of operations of the rate enforcement algorithm. It takes a value of 0 or 1 only
Customer Edge	Equipment on the Subscriber side of the UNI
CIR	Committed Information Rate
CIR-compliant	Service frames that are compliant with the CIR of the bandwidth profile. CIR-compliant service frames are colored green.
Circuit Emulation Service	A service that transports TDM-based traffic over a Metro Ethernet Network.
Class of Service	A set of Service Frames that have a commitment from the Service Provider to receive a particular level of performance.
CLI	Command Line Interface
CM	Configuration Management
Color-aware	A traffic management capability used to determine whether traffic is conformant or non-conformant to a bandwidth profile based on different CoS ID values.
Color-blind	A traffic management capability that ignores a CoS ID value that may have been changed to indicate that traffic was conformant or non-conformant to a bandwidth profile.
Committed Burst	The maximum number of bytes that can be sent at the UNI speed and be CIR-compliant.

Term	Definition
Size	
Committed Information Rate	CIR is a Bandwidth Profile parameter. It defines the average rate in bits/s of ingress Service Frames up to which the network delivers Service Frames and meets the performance objectives defined by the CoS Service Attribute.
CoS	Class of Service
Current Problem List	Identifies the current existing problems (probable cause), with severity for an entity
Customer	The organization purchasing and/or using Ethernet Services. Alternate term: Subscriber
Customer Edge	Equipment on the Subscriber side of the UNI
Customer Edge VLAN CoS	The 802.1p user priority bits in the IEEE 802.1Q Tag in a tagged Service Frame.
Customer Edge VLAN ID	The identity of the VLANs on the Ethernet port of the customer equipment that is attached to the UNI.
Customer Edge VLAN Tag	The IEEE 802.1Q Tag in a tagged Service Frame. When present, it contains the customer Edge VLAN ID and the Customer Edge VLAN CoS.
Dual Rate Bandwidth Profile	A bandwidth profile that specifies both a CIR/CBS and EIR/EBS.
EBS	Excess Burst Size
Egress Service Frame	A service frame sent from the Service Provider network to the CE.
E-NNI	External Network to Network Interface
EIR	Excess Information Rate
EIR-compliant	Service frames that are compliant with the EIR of the bandwidth profile. EIR-compliant service frames may be colored green or yellow depending upon whether they are CIR-compliant or not, respectively.
E-LMI	Ethernet Layer Management Interface
E-NNI	External Network to Network Interface
ETH FPP	An Ethernet Flow Point Pool that represents an Ethernet UNI or E-NNI.
Ethernet Virtual Connection	An association of two or more UNIs that limits the exchange of frames to UNIs in the Ethernet Virtual Connection
ETY	Ethernet Physical Layer
EVC	Ethernet Virtual Connection
Excess Burst Size	EBS is a Bandwidth Profile parameter. It limits the maximum number of bytes available for a burst of ingress Service Frames sent at the UNI speed to remain EIR-conformant.
Excess Information Rate	EIR is a Bandwidth Profile parameter. It defines the average rate in bits/s of ingress Service Frames up to which the network may deliver Service Frames without any performance objectives.
FD	Frame Delay
FDX	Full Duplex
Frame	Short for Ethernet frame.
Frame Delay	The time required to transmit a Service Frame from source to destination across the metro Ethernet network.
Frame Delay Performance	A measure of the delays experienced by different Service Frames belonging to the same CoS instance.
Frame Delay Variation	The difference in delay of two Service Frames.
Frame Delay Variation Performance	A measure of the variation in the delays experienced by different Service Frames belonging to the same CoS instance.
Frame Loss Ratio Performance	Frame Loss Ratio is a measure of the number of lost frames in-side the MEN. Frame Loss Ratio is expressed as a percentage.
HDX	Half Duplex
IE	Information Element

Term	Definition
Ingress Frame	A service frame sent from the CE to the Service Provider network.
Layer 2 Control Protocol Service Frame	A Service Frame that is used for Layer 2 control, e.g., Spanning Tree Protocol.
Layer 2 Control Protocol Tunneling	The process by which a Layer 2 Control Protocol Service Frame is passed through the Service Provider network switches without being processed by those switches and delivered to the proper UNI(s).
MEN	Metro Ethernet Network
ME-NE	Metro Ethernet Network Element
Metro Ethernet Network	The service provider's network providing metro Ethernet services.
Metro Ethernet Network Element	A Network Element supporting Metro Ethernet services
MTTR	Mean Time To Restore
Multicast Service Frame	A Service Frame that has a multicast destination MAC address.
Multipoint-to-Multipoint EVC	An EVC with two or more UNIs. A Multipoint-to-Multipoint EVC with two UNIs is different from a Point-to-Point EVC because one or more additional UNIs can be added to it.
N/S	Not Specified
Point-to-Point EVC	An EVC with exactly 2 UNIs.
Service Frame	An Ethernet frame transmitted across the UNI toward the Service Provider or an Ethernet frame transmitted across the UNI toward the Subscriber.
Service Level Agreement	The contract between the Subscriber and Service Provider specifying the agreed to service level commitments and related business agreements.
Service Level Specification	The technical specification of the service being offered by the Service Provider to the Subscriber.
Service Multiplexing	A UNI attribute in which the UNI can be in more than one EVC instance
Service Provider	The organization providing the Ethernet service(s).
SLA	Service Level Agreement
SNI	Service Node Interface
Subscriber	The organization purchasing and/or using Ethernet Services. Alternate term: Customer
SLS	Service Level Specification
UNI	User Network Interface
Unicast Service Frame	A Service Frame that has a unicast destination MAC address
UNI-C	The functional elements within the Customer Edge that supports the MEN Subscriber's technical capabilities and compliance to the UNI specification
UNI-N	A set of one or more functional elements that supports the MEN Service Provider's technical capabilities and compliance to the UNI specification
User Network Interface	The demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber.
VLAN	Virtual LAN

3. Scope

This draft specification focuses on what is considered to be the essential network management functionality of Metro Ethernet Network Elements (ME-NEs) supporting Ethernet Service Phase 1 as defined in MEF10 [2]. The ME-NE is a Provider Edge network element supporting carrier class Ethernet Services. This specification sets forth operations requirements necessary to support Phase 1 Metro Ethernet services at the ME-NE. Requirements are stated for the management of interfaces (e.g., User-Network Interface (UNI)), Ethernet Virtual Connections (EVCs / Flow Domain Fragments), and EVC endpoints (Flow Points).

This version of the MEF Network Element Management Requirements provides management requirements supporting other MEF work:

- Ethernet services and service attributes defined to date MEF10 [2]
- UNI Types 1 [MEF11]
- Performance Measurements

Additional requirements supporting management mechanisms (e.g., OAM, E-LMI), Service Phase 2, etc. will be defined in subsequent specifications.

The core management functionality covered in this specification is grouped into four functional categories: Configuration Management, Fault Management, Performance Management, and Security Management. Configuration Management refers to the set of functions closely associated with network and service provisioning as well as the administration of the configuration of a ME-NE. Performance Management and Fault Management functions are designed to maintain the MEN. This includes the maintenance of ME-NEs, ME-NE components, transport terminations, and EVCs. In addition, the Performance Data Collection requirements defined are needed to gather data to support network capacity planning and engineering purposes.

4. 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. All key words must use upper case, bold text.

5. General Requirements

These general ME-NE requirements describe functionality that spans four functional categories: Configuration Management, Fault Management, Performance Management, and Security Management.

5.1 MANAGEMENT INTERFACE REQUIREMENTS

Management interfaces (e.g., NE-EMS) provide an open means by which management systems can directly or indirectly communicate with and manage various elements within the ME-NE. In addition to managing the ME-NE via an automated interface, direct user interfaces may also be supported.

Requirements Group 1. Management Interface

- R 1.1.** A ME-NE **SHALL** communicate with the managing systems (e.g., EMS or NMS) by means of a well-defined standards based management interface using an industry accepted management protocol (e.g., SNMP, TL/1, CORBA, CMIP, XML SOAP, etc.).
- R 1.2.** In order to support file-oriented communications, the ME-NE **SHOULD** use File Transfer Protocol (FTP) or Trivial File Transfer Protocol (TFTP).

5.2 TRANSPORT LAYER INTERFACES

The ME-NE may support various types of transport terminations that are used by the ETH layer as a server layer for the transport of ETH frames as payload. The focus of this specification is on the aspects of the ME-NE that deal with Metro Ethernet Service functionality. Details of transport level management are outside the scope of this specification.

Requirements Group 2. Transport Layer Interface Management

- R 2.1.** For each transport connection that terminates on the ME-NE, the ME-NE **SHOULD** support the appropriate standards based management functions.

6. Configuration Management Requirements

Configuration Management (CM) deals with the initialization, maintenance, and graceful shutdown of resources within a system. Configuration information is defined and managed (created, retrieved, updated, and deleted) using Configuration Management functions. Software distribution, memory backup and recovery, and maintaining the configuration status are other primary functions of Configuration Management.

6.1 UPDATE NOTIFICATIONS

Requirements Group 3. Notification of Local CM Activity and State Changes

The ME-NE must be capable of recognizing when a local change has been made to its configuration and notify the managing system (EMS or NMS) of this change.

- R 3.1.** The ME-NE **SHALL** report to the managing system whenever the ME-NE autonomously detects a new component, interface card, or other hardware using an object creation notification.
- R 3.2.** The ME-NE **SHALL** report to the managing system whenever the ME-NE autonomously detects a component, interface card, or other hardware is removed using an object deletion notification.
- R 3.3.** The ME-NE **SHALL** report to the managing system (using object creation / deletion notification, state change notification, attribute value change notification, and relationship change notification) when it detects changes made to its configuration information database resulting from local CM activity, i.e., CM actions initiated by operations personnel or systems other than the managing system via its CLI (Command Line Interface) or other operations interfaces.

- R 3.4.** The ME-NE **SHALL** report to the managing system when the ME-NE has been installed or initialized and is available for subsequent provisioning.
- R 3.5.** The ME-NE **SHALL** report to the managing system using a state change notification when the operational state of any of its managed entities has changed.
- R 3.6.** The ME-NE **SHOULD** support the enabling or disabling of events/notifications on both a per-event type and a per-resource basis.

6.2 CONFIGURATION BACKUP AND RECOVERY

Requirements Group 4. Configuration Backup and Restoration

The ME-NE needs to be able to restore its configuration database to the last known stable condition in the case of the corruption of configuration data.

- R 4.1.** The ME-NE **SHALL** create a backup of configuration data by downloading stable data to nonvolatile storage located either on the ME-NE or on a remote server.
- R 4.2.** The ME-NE **SHALL** save updates and changes to the latest archive of configuration data and the ME-NE **SHALL** maintain a backup of this configuration change data.
- R 4.3.** The ME-NE **SHALL** restore configuration data from a backup following the detection of corrupted data in the configuration database.
- R 4.4.** The ME-NE **SHALL** restore configuration data from a backup upon receiving a request to do so by the managing system.

6.3 NETWORK PROVISIONING AND INSTALLATION

Requirements Group 5. Network Element Installation

- R 5.1.** If the management mechanism for the ME-NE is supported by IP, the ME-NE **SHALL** be configured with an IP address for the ME-NE to be used for management purposes.
- R 5.2.** A ME-NE **SHOULD** be configured with the network address of its managing systems for the purpose of forwarding notifications/events and accepting management instructions.
- R 5.3.** A ME-NE **SHALL** be configured with a name (e.g., an 11-character CLI code or textual name managed by the carrier) by which the ME-NE will be known.
- R 5.4.** A ME-NE **SHOULD** be configured with a geographic location for the ME-NE. (A geographic location will be needed to properly position the NE on geographic maps.) For example, the first 8 characters of the CLI code may be used to describe the NE location.
- R 5.5.** A ME-NE **SHOULD** be configured with time of day. Configuration of the time zone is OPTIONAL.

- R 5.6.** A ME-NE **SHOULD** be able to periodically adjust the local date and time value from an external time source, preferably using NTP (RFC 1305).
- R 5.7.** If the date and time adjustment functionality is supported, the ME-NE **SHALL** allow this functionality to be enabled or disabled.
- R 5.8.** If the date and time adjustment functionality is supported, the ME-NE **SHALL** allow the configuration of a number of separate time sources, so that a failure in a single time source does not prevent the adjustment.

Requirements Group 6. Software Loading

The ME-NE needs to be able to receive software, activate it, and maintain a record of the version of the software it is running.

- R 6.1.** Upon request by the managing system to perform a software download, the ME-NE **SHALL** be capable of initiating the transfer of the software image either from the managing system, or from a location specified by the managing system.
- R 6.2.** All software downloads **SHALL** be performed without halting or rebooting the ME-NE.
- R 6.3.** The ME-NE **SHOULD** be capable of loading software images to specific components (e.g., line cards) at a specified time or immediately.
- R 6.4.** The ME-NE **SHALL** maintain a record of the software images(s) it is running including the following attributes:
- Supplier name
 - Software title
 - Version number
 - Release (OPTIONAL)
 - Date of software image load onto the ME-NE
 - Patches or service packs activated
- R 6.5.** The ME-NE **SHALL** be capable of receiving the software images to be loaded.
- R 6.6.** The ME-NE **SHALL** activate a software load upon receiving a request to do so from a managing system.
- R 6.7.** Software downloads **SHALL** be done without interrupting services for subscribers.
- R 6.8.** The software **SHOULD** be automatically activated on the ME-NE once the correctness of it has been verified. This load **SHOULD** occur immediately or at a pre-defined time.
- R 6.9.** The ME-NE **SHALL** send a confirmation to the managing system that it has been successful in its attempt to activate the software load once a stable state is reached after activation.
- R 6.10.** The ME-NE **SHALL** retain the previous version of the software, so that the software may be reverted to the previous version without having to download the previous version.

- R 6.11.** If the ME-NE has a component that requires programmable software (e.g., plug-in, circuit pack, etc.), it **SHALL** be capable of loading and activating a software on a per-component basis.
- R 6.12.** The ME-NE **SHOULD** provide download operation states to the managing system. In addition changes to these states **SHOULD** be logged.

Requirements Group 7. Management of ME-NE Configuration Data

- R 7.1.** The following ME-NE data **SHALL** be available for retrieval and/or modification:
- Network Element Name
 - Flow Domain (e.g., the management flow domain)
 - User Label (e.g., CLI or hostname)
 - Supplier Name (read-only)
 - Model (read-only)
 - Serial Number (read-only)
 - Version (read-only)
 - Location
 - Administrative State (used to lock and unlock the NE. A locked NE is not active from a network services perspective, but still allows the management interactions.)
 - Operational State (enabled or disabled, read-only)
 - The reason the operational state is disabled (if it is disabled)
 - External Time (NTP or wall-clock time used for notifications, etc.)
- R 7.2.** The following properties of the ME-NE **SHALL** be available for retrieval and/or modification:
- Equipment composing the ME-NE (equipment bays, shelves, etc.)
 - Ports on the ME-NE
 - Transport Link terminations on the ME-NE
 - Software installed on the ME-NE
 - An alarm severity assignment profile, detailing the severity assigned to different types of alarms emitted from the ME-NE (**OPTIONAL**)
 - Performance threshold profile, detailing the performance limits at which threshold crossing alerts are emitted for the ME-NE (**OPTIONAL**)
 - EVCs terminating at the ME-NE
 - MEF interfaces on the ME-NE
 - ETH Flow points terminating on the ME-NE
- R 7.3.** Any changes to the ME-NE configuration **SHALL** be logged.
- R 7.4.** Any operation that violates a network resource entity relationship or causes an invalid state transition **SHALL NOT** be allowed.
- R 7.5.** The ME-NE **SHALL** report any invalid states to the managing system.

Requirements Group 8. Installation Testing

- R 8.1.** The ME-NE **SHALL** supply the managing system with a list of available installation tests (self-tests) that are supported on the ME-NE.
- R 8.2.** The ME-NE **SHALL** be capable of performing installation tests (self-tests) when invocation is requested and upon system initialization. The actual tests available will depend on the tests supported by the NE.
- R 8.3.** The ME-NE **SHALL** allow invocation of available installation tests on the console interface, the craft interface and via the managing system.
- R 8.4.** The ME-NE **SHALL** report the results of completed installation tests.

Requirements Group 9. Circuit Pack Resource Management

- R 9.1.** Upon the installation of a new piece of equipment into an ME-NE, such as a circuit pack, the ME-NE **SHALL** automatically detect the addition and notify the managing system with all relevant data about the new equipment.
- R 9.2.** If a compatible piece of equipment had previously been installed in this same location, the ME-NE **SHOULD** automatically configure the new equipment the same way the old equipment was configured. This is to automate the handling of cases where a piece of defective equipment is removed and a new piece installed.
- R 9.3.** Upon equipment replacement, if the equipment had previously supported any EVCs that are now disabled (i.e., in a failure state), the ME-NE **SHOULD** be configurable for automatic or manual enablement of such EVCs.
- R 9.4.** The ME-NE **SHALL** log any changes to its plug-in resources.
- R 9.5.** If the addition of the equipment consumes a resource such as a slot in a shelf, and this addition crosses a pre-set threshold set for that resource, the ME-NE **SHALL** generate a threshold crossing alert to notify the managing system.
- R 9.6.** The following data about the plug-in unit **SHOULD** be viewed and modified:
- Plug-in Unit Name
 - User Label
 - Supplier Name (read-only)
 - Equipment Code (e.g., CLEI) (**OPTIONAL**)
 - Function Code (e.g., HECI) (**OPTIONAL**)
 - Version (read-only)
 - Serial Number (read-only)
 - Administrative State (used to lock and unlock the plug-in unit. A locked plug-in unit is not active.)
 - Operational State (enabled or disabled, read-only)
 - Alarm Status
 - Current Problem List
 - Availability Status (inTest, failed, powerOff, degraded, notInstalled, read-only)

— List of Ports on the plug-in unit.

- R 9.7.** Upon the removal of a piece of equipment from a ME-NE, such as a circuit pack, the ME-NE **SHALL** automatically detect and report the removal.
- R 9.8.** The ME-NE **SHALL** treat any service related entities supported by removed equipment as if the equipment failed. Alarms are generated; the services are shown as disabled.
- R 9.9.** The ME-NE **SHOULD** automatically store the configuration of the removed equipment so that if a compatible new piece is installed it may be automatically configured the same as the old.

Requirements Group 10. Transport Layer Port Configuration

The Transport Layer Port generically represents the underlying transport termination (e.g., DS3, SONET, SDH etc.). An instance of ETH FPP (UNI or E-NNI) may be associated with a Transport Layer Port to represent the association between an interface and the transport supporting facility. Usually a Transport Layer Port supports a single ETH FPP (UNI or E-NNI), however if MEF Transport Multiplexing Function is used, it is possible that multiple ETH UNIs may be supported from a single Transport Layer Port

- R 10.1.** The ME-NE **SHALL** maintain the following information about each Transport Layer Port:
- Characteristic Information Type: describes the transport type provided by the Transport Layer Port
 - Operational State
 - Alarm Status
 - Current Problem List
 - Port ID (Unique within the scope of the ME-NE)
 - Potential Capacity (**OPTIONAL**)
 - Assigned Capacity (**OPTIONAL**)
- R 10.2.** The ME-NE **SHALL** support automatic creation of the Transport Layer Port whenever an equipment entity supporting the Transport Layer Port is instantiated
- R 10.3.** The ME-NE **SHALL** support the deletion of a Transport Layer Port, only if no ETH_FPPs are associated with the Transport Layer Port to be deleted.
- R 10.4.** The ME-NE **SHOULD** emit notifications when a Transport Layer Port is created or deleted.
- R 10.5.** The ME-NE **SHOULD** maintain a relationship between the Transport Layer Port and an alarm severity profile in order to assign alarm severity to specific alarms.
- R 10.6.** The ME-NE **SHALL** maintain a relationship between the Transport Layer Port and the elements (e.g., circuit packs) that support the Transport Layer Port.
- R 10.7.** The ME-NE **SHALL** maintain a relationship between the Transport Layer Port and the FPP in the client layer supported by the Transport Layer Port.

Requirements Group 11. MAU Transport Termination Configuration

- R 11.1.** For each Transport Layer Port that represents the underlying transport termination of the Ethernet Medium Attachment Unit, the ME-NE **SHALL** maintain the following information about each MAU Transport Termination:
- Operational State
 - Alarm Status
 - Current Problem List
 - Port ID (Unique within the scope of the ME-NE)
 - Potential Capacity (**OPTIONAL**)
 - MAU Type (as defined in RFC-3636)
 - MAU Media Available (link integrity state of the MAU TTP. May take on the following values as describe in RFC-3636: other, unknown, available, notAvailable, remoteFault, invalidSignal, remoteJabber, remoteLinkLoss, remoteTest, offline, autoNegError, pmdLinkFault, wisFrameLoss, wisSignalLoss, pcsLinkFault, excessiveBER, dxsLinkFault, and pxsLinkFault)
 - MAU Jabber State (may take on the following values as described in RFC-3636: other, unknown, noJabber, and jabbering)
 - MAU Default Type (identifies the default administrative baseband MAU type, to be used in conjunction with the operational MAU type denoted by mauType)
 - Mode (Full Duplex, or Auto negotiation)
 - MAU Auto-negotiation supported
 - MAU Type List (set of possible IEEE 802.3 types that the MAU could be)
 - MAU Jack Type List (the set of possible interface jack types that the MAU provides. Values include: other, rj45, rj45S, db9, bnc, fAUI. Based on RFC-3636 ifJackTable)
 - MAU Auto-negotiation Admin State (allows the auto-negotiation function of the MAU to be enabled or disabled)
 - MAU Auto-negotiation Remote Signaling (allows the auto-negotiation function of the MAU to be enabled or disabled)
 - MAU Auto-negotiation Config (indicates the current status of the auto-negotiation process. May take on the following values as describe in RFC-3636: other, configuring, complete, disabled, or parallelDetectFail)
 - MAU Auto-negotiation Capability (identifies the set of capabilities of the local auto-negotiation entity)
 - MAU Auto-negotiation Capabilities Advertised (identifies the set of capabilities advertised by the local auto-negotiation entity)
 - MAU Auto-negotiation Capabilities Received (identifies the set of capabilities received from the remote auto-negotiation entity)
 - MAU Auto-negotiation Remote Fault Advertised (identifies any local fault indications that this MAU has detected and will advertise at the next auto-negotiation interaction. May take on the following values as describe in RFC-3636: noError, offline, linkFailure, or autoNegError)
 - MAU Auto-negotiation Remote Fault Received (identifies any fault indications received from the far end of a link by the local auto-negotiation entity. May take on the following values as describe in RFC-3636: noError, offline, linkFailure, or autoNegError)

- R 11.2.** For each Transport Layer Port that represents the underlying transport termination of the Ethernet Medium Attachment Unit, the ME-NE **SHALL** allow updates to the MAU Auto-negotiation Admin State.
- R 11.3.** The ME-NE **SHALL** support automatic creation of the MAU Transport Termination whenever an equipment entity supporting the MAU Transport Termination is instantiated
- R 11.4.** The ME-NE **SHALL** support the deletion of a MAU Transport Termination, only if no ETH_FPPs are associated with that MAU Transport Termination.
- R 11.5.** The ME-NE **SHOULD** emit notifications when a MAU Transport Termination is created or deleted.
- R 11.6.** The ME-NE **SHOULD** maintain a relationship between the MAU Transport Termination and an alarm severity assignment profile in order to assign alarm severity to specific alarms).
- R 11.7.** The ME-NE **SHALL** emit notifications when a MAU Transport Termination is created or deleted.

6.4 SERVICE ACTIVATION

The functions under Service Activation are used to configure the equipment to provide service. Once the equipment has been installed and the software and initial installation configuration data has been loaded, Service Activation must be performed. Service Activation ensures that the ME-NE receives the data necessary in order to use resources to provide the intended network service.

Requirements Group 12. Bandwidth Profile Management

- R 12.1.** The ME-NE **SHALL** maintain the following information as part of the MEF Bandwidth Profile:
- Bandwidth Profile Identifier
 - Committed Information Rate (CIR) in bits per second
 - Committed Burst Size (CBS) in bytes
 - Excess Information Rate (EIR) in bits per second
 - Excess Burst Size (EBS) in bytes
 - Color Mode (CM) to be applied (i.e., color-blind mode or color-aware mode)
 - Coupling Flag (CF), describes if yellow frames will be admitted if unused bandwidth is available (**OPTIONAL**)
- R 12.2.** The ME-NE **SHALL** support the creation of new MEF Bandwidth Profiles.
- R 12.3.** The ME-NE **SHALL** support the deletion of a MEF Bandwidth Profile, only if no termination points are associated with the MEF bandwidth profile to be deleted.
- R 12.4.** The ME-NE **SHOULD** emit notifications when a MEF Bandwidth Profile is created or deleted.

Requirements Group 13. ETH Interface Configuration

ETH Flow Point Pools (FPPs) represent interfaces, MEF UNIs or E-NNIs, at the ETH Layer. An ETH FPP consists of a subset of the ETH flow points at the edge of one ETH flow domain (on the ME-NE) that are associated through the ETHLink with a corresponding subset of ETH flow points at the edge of another ETH flow domain (on another ME-NE) for the purpose of transferring ETH characteristic information (ETH Frames).

- R 13.1.** The ME-NE **SHALL** maintain the following information about each ETH Flow Point Pool:
- FPP Type: Indicates that the ETH_FPP is a UNI, E-NNI, SNI, or Unconfigured
 - FPP total bandwidth capacity
 - Per CoS FPP total bandwidth capacity (**OPTIONAL**)
 - User Label (e.g., Circuit ID of associated transport circuit)
 - IEEE 802.3 address
 - Operational State
 - Availability Status (inTest, failed, degraded, notInstalled, read-only)
 - Administrative State
 - Maximum amount of assignable bandwidth on the interface in the Ingress direction
 - Maximum amount of assignable bandwidth on the interface in the Egress direction
 - Per CoS Maximum amount of assignable bandwidth on the interface in the Ingress direction (**OPTIONAL**)
 - Per CoS Maximum amount of assignable bandwidth on the interface in the Egress direction (**OPTIONAL**)
 - Maximum number of virtual connections (FDFrs/EVCs)
 - Number of currently configured virtual connections (FDFrs/EVCs)
 - Usage cost allocated to the Link supported by the interface (**OPTIONAL**)
- R 13.2.** The ME-NE **SHALL** support the creation of new ETH_FPPs upon request from a managing system.
- R 13.3.** The ME-NE **SHOULD** support automatic creation of the ETH_FPP whenever an equipment entity supporting ETH ports is instantiated. In this case, FPP Type **SHOULD** initially be set to Unconfigured.
- R 13.4.** The ME-NE **SHALL** support the deletion of a ETH_FPP, only if no termination points are associated with that ETH_FPP.
- R 13.5.** The ME-NE **SHOULD** emit notifications when a ETH_FPPs is created or deleted.
- R 13.6.** The ME-NE **SHALL** allow updates to the following information about each ETH Flow Point Pool:
- FPP Type: Indicates that the ETH_FPP is a UNI, E-NNI, SNI, or Unconfigured (FPP Type shall only be updated when no termination points are associated with the ETH_FPP)
 - User Label (e.g., Circuit ID of associated transport circuit)
 - IEEE 802.3 address
 - Maximum number of virtual connections (FDFrs/EVCs)
 - Usage cost allocated to the Link supported by the interface (**OPTIONAL**)

- R 13.7.** The ME-NE **SHALL** maintain a relationship between the ETH_FPP and the elements (e.g., circuit packs) that support the ETH_FPP.
- R 13.8.** The ME-NE **SHALL** maintain a relationship between the ETH_FPP and the supporting TRANS (could be ETH layer Flow Point for tunneling, a TransportPort, etc.) layer termination point.
- R 13.9.** The ME-NE **SHALL** maintain a relationship between the ETH_FPP and the Flow Points that terminate on the ETH_FPP.

Requirements Group 14. ETH UNI Configuration

This requirements group describes additional requirements for ETH interfaces (ETH_FPPs) configured as ETH UNIs.

- R 14.1.** For each ETH_FPP that is configured as a UNI, the ME-NE **SHALL** maintain the following information about each ETH_FPP_UNI:
- UNI Identifier (service provider assigned)
 - A list of the possible Layer 2 Control protocols processed at this UNI interface. Each entry in this list shall describe the control protocol and provide the corresponding destination MAC address along with the processing alternative (Discard, Peer, Pass-to-EVC) – if pass to EVC, EVC shall be identified
 - Service Multiplexing Indicator
 - Bundling Indicator
 - All-to-One Bundling Indicator
 - CE-VLAN-ID assigned to untagged and priority tagged traffic (An integer from 1 to 4094 inclusive)
 - List of unique values that are available for assignment as the Customer Edge VLAN ID (CE-VLAN ID) when creating new EVCs (**OPTIONAL**)
 - Next available CE-VLAN ID (**OPTIONAL**)
 - OAM Domain Information (FFS)
- R 14.2.** For each ETH_FPP that is configured as a UNI, the ME-NE **SHALL** allow updates to the following information about each ETH_FPP_UNI:
- UNI Identifier (service provider assigned)
 - A list of the possible Layer 2 Control protocols processed at this UNI interface. Each entry in this list shall describe the control protocol and provide the corresponding destination MAC address along with the processing alternative (Discard, Peer, Pass-to-EVC)
 - Service Multiplexing Indicator
 - Bundling Indicator
 - All-to-One Indicator
 - CE-VLAN-ID assigned to untagged and priority tagged traffic (An integer from 1 to 4094 inclusive)
 - OAM Domain Information (FFS)
- R 14.3.** For each ETH_FPP that is configured as a UNI, the ME-NE **SHALL** maintain a relationship between the ETH_FPP and the ingress bandwidth profiles that characterize the

ETH_FPP_UNI in the ingress direction. This association **MUST** be performed according to the rules specified in [MEF-10]

Requirements Group 15. EVC Flow Point Configuration

An EVC Flow Point represents the termination of an EVC at the edge of an ETH_Flow_Domain.

R 15.1. The ME-NE **SHALL** maintain the following information about each EVC_Flow_Point:

- Administrative State
- Operational State
- Availability Status: The availability status attribute is read only and indicates that the ETH_FDFr_EVC is functioning properly. May be mapped to IETF's rfc 2863, The Interfaces Group MIB IfOperStatus. Values for availability status include: inTest, failed, degraded.
- Alarm Status
- Current Problem List
- ethEVCID: The ethEVCID attribute represents a unique identifying value for the ETH Virtual Connection
- EVC Type (Describes the ETH EVC as: Connection_MultipointToMultipoint, Connection_PointToPoint)
- User Label: A text string that may be used to provide additional information about the ETH_FDFr_EVC, such as a circuit identifier
- EVC Protected: This attribute indicates if the ETH_FDFr_EVC is protected or not at the ETH layer (OPTIONAL)
- CE VLAN Id Preservation: This Boolean attribute identifies an EVC where the CE VLAN IDs of egress frames are always identical to the CE VLAN IDs of the corresponding ingress frames as per [MEF-10].
- UNI CE VLAN COS Preservation: This Boolean attribute identifies an EVC where the CE VLAN COS user_priority bits of an egress frame is always identical to the CE VLAN COS user_priority bits of the corresponding ingress frame.
- CE VLAN ID Mapping: A list of unique values that map each Customer Edge VLAN ID (CE-VLAN ID) to at most one EVC
- Interface (e.g., UNI, E-NNI) EVC Identifier (identifies the EVC that the Flow Point terminates at the containing interface)
- Layer 2 Control Protocol Disposition List (a list that describes Layer 2 control protocols, along with the frame disposition for each potential destination: Discard or Tunnel)
- Service frame delivery attribute for Unicast Service Frames (Describes the service frame delivery option for Unicast Service Frames as: Discard, DeliverUnconditionally, or DeliverConditionally¹)
- Service frame delivery option for Multicast Service Frames (Describes the service frame delivery option for Multicast Service Frames as: Discard, DeliverUnconditionally, or DeliverConditionally)

¹ Deliver Conditionally includes condition that must be specified. An example of such a condition is that the destination MAC address is known by the Metro Ethernet Network to be "at" the destination UNI. Another example is broadcast throttling where some Service Frames with the broadcast destination MAC address are dropped to limit the amount of such traffic.

- Service frame delivery option for Broadcast Service Frames (Describes the service frame delivery option for Broadcast Service Frames as: Discard, DeliverUnconditionally, or DeliverConditionally)
 - Trail Terminating Indicator: Boolean. If TRUE, describes Flow Point as a point where frame flow terminates (i.e., a G.809 TFP) and is adapted into the APP layer. Otherwise shall be set to FALSE.
- R 15.2.** The ME-NE **SHALL** support requests for the creation of new EVC_Flow_Points.
- R 15.3.** The ME-NE **SHALL** support requests for the deletion of a EVC_Flow_Point.
- R 15.4.** The ME-NE **SHOULD** emit notifications when a EVC_Flow_Point is created or deleted.
- R 15.5.** The ME-NE **SHALL** allow updates to the following information about each ETH Flow Point:
- Administrative State
 - CE VLAN ID Mapping: A list of unique values that map each Customer Edge VLAN ID (CE-VLAN ID) to at most one EVC
 - Interface (e.g., UNI, E-NNI) EVC Identifier
 - Layer 2 Control Protocol Disposition List
 - Service frame delivery option for Unicast Service Frames
 - Service frame delivery option for Multicast Service Frames
 - Service frame delivery option for Broadcast Service Frames
 - UNI CE VLAN Id Preservation
 - UNI CE VLAN COS Preservation
- R 15.6.** The ME-NE **SHALL** maintain a relationship between the EVC_Flow_Point and ETH_FPP (UNI or E-NNI) in which it is contained.
- R 15.7.** The ME-NE **MAY** maintain a relationship between the EVC_Flow_Point and an alarm severity profile in order to assign alarm severity to specific alarms).
- R 15.8.** The ME-NE **SHALL** maintain a relationship between the EVC_Flow_Point and ETH FDFr EVC which it terminates.
- R 15.9.** The ME-NE **SHALL** maintain a relationship between the EVC_Flow_Point and bandwidth profile in the ingress direction (single, or one per COS set). The association **MUST** be performed according to the rules specified in MEF 10[2]
- R 15.10.** The ME-NE **SHOULD** maintain a relationship between the EVC_Flow_Point and an alarm severity profile in the ingress direction (one for each COS set), if configured.
- R 15.11.** When adaptation is provided at the EVC_Flow_Point, the ME-NE **SHALL** maintain a relationship between the (trail terminating) EVC_Flow_Point and the adaptation profile that provides necessary adaptation parameters.
- R 15.12.** The ME-NE **SHALL** maintain a relationship between the EVC_Flow_Point and the ingress CoS profiles that is acting as the client layer in the client/ server relationship.
- R 15.13.** When ETH tunneling is terminated at the EVC_Flow_Point, the ME-NE **SHALL** maintain a relationship between the (trail / tunnel terminating) EVC_Flow_Point and the ETH_FPP_UNI that is the client layer termination associated with the tunnel (server layer).

6.5 STATUS MANAGEMENT AND CONTROL

The functions under Status Management and Control provide for the ability of operations management to monitor and control certain aspects of the network on demand. These functions may be invoked to determine the current state of ME-NE resources.

Requirements Group 16. Autonomous Notification of State Changes

R 16.1. The ME-NE **SHALL** report state change notifications that reflect changes in the operational state of its managed entities. When possible, only the root operational state change **SHALL** be reported (i.e., operational state changes that may be derived from the root state change should not be reported).

Requirements Group 17. Logging of State Changes

R 17.1. The ME-NE **SHALL** maintain a time-stamped log of all changes in operational state and administrative, and make this information available (on-demand) over the operations interface.

R 17.2. The state change log **SHOULD** be maintained in a non-volatile rolling buffer.

R 17.3. The state change log **SHOULD** be retrievable by a managing system by a specified range of timestamps within the retention interval.

Requirements Group 18. Activating / Deactivating ME-NE Functions

A management system may exercise control over a ME-NE by activating and deactivating the various functions the ME-NE performs. In support of this capability, the ME-NE must allow authorized management systems to lock (deactivate) and unlock (activate) functionality in the ME-NE.

R 18.1. An ME-NE **MUST** allow authorized management systems to activate/deactivate (i.e., unlock/lock) manageable functions of the ME-NE, including:

- Sub-ME-NE components (e.g., circuits packs and equipment modules)
- Transport terminations (ports), which includes transmission level (Section, Line, Path) functions
- Logging functions
- Performance data collection activities
- Services

7. Fault Management Requirements

Fault Management functions handle the detection and isolation of faults and the repair of failed components. A fault condition occurs when a resource fails to function correctly or when an excessive number of errors occur. In addition to the detection and reporting of failures, Fault Management assists in the isolation and diagnosing of faults. This includes performing tests, such as connectivity tests, integrity tests, response time tests, diagnostic tests, etc.

7.1 ALARM SURVEILLANCE

Alarm surveillance provides the capability to monitor failures detected in NEs in near real time. This information, along with other information allows the Network Manager to determine the nature and severity of the fault. The term ‘alarm’ actually refers to all types of fault events that are associated with a potential failure.

Requirements Group 19. Alarm Reporting Control

Alarm reporting control enables a user to control how alarms are processed by the managing system.

- R 19.1.** The ME-NE **SHOULD** allow the “soaking” intervals (i.e. alarm hold-down timer) for the various alarm conditions to be set. A soaking interval defines how long a condition must persist before an alarm is declared.
- R 19.2.** The ME-NE **SHOULD** allow the “soaking” intervals (i.e. alarm hold-down timer) for the various alarm conditions to be cleared. A soaking interval defines how long a clearing condition must persist before an alarm is cleared.
- R 19.3.** The ME-NE **SHALL** allow a default alarm severity profile to be assigned automatically upon initialization and used by the ME-NE to assign alarm severity (e.g., Critical, Major, Minor, Warning) to failure conditions for the resources on the NE that provide alarm notifications.
- R 19.4.** The ME-NE **SHALL** allow the assignment of alarm severity for specific types of network resources that provides alarm notifications on a per resource type basis.

Requirements Group 20. Alarm Monitoring

- R 20.1.** Upon the detection of alarm conditions, the ME-NE **SHALL** generate an alarm notification and forward that message to the managing systems.
- R 20.2.** Upon the clearing of an alarm condition, the ME-NE **SHALL** generate a clear notification and forward that notification to the managing systems.
- R 20.3.** The ME-NE **SHALL** allow the managing systems to manage alarm filters based on component ID, severity, and alarm classification.
- R 20.4.** The ME-NE **SHALL** include in the alarm notifications sufficient information to help isolate failed replaceable units.
- R 20.5.** The ME-NE **SHALL** support queries for alarm status and state information.
- R 20.6.** The ME-NE **SHALL** generate an alarm condition upon the occurrence of any of the following failure conditions:
 - Power loss
 - Environmental condition not conducive to normal operation (e.g., temperature)
 - Loss of data integrity (e.g., equipment failure)

- R 20.7.** The ME-NE **SHALL** monitor, detect and generate alarm conditions and states associated with hardware components of the ME-NE.
- R 20.8.** The ME-NE **SHALL** monitor, detect and generate alarm conditions and states associated with software/process state.
- R 20.9.** The ME-NE **SHALL** monitor, detect and generate alarms conditions and states associated with ME-NE interfaces.
- R 20.10.** Upon the failure of the interface between management system (including the EMS and NMS) and the ME-NE, the ME- NE **SHALL** be capable of storing related management information such as event and alarm notifications until the interface is operational. Once the interface is operational the ME-NE **SHALL** make available to the managing system the temporarily stored management information
- R 20.11.** Alarm notifications **SHALL** be identified as one of the following classifications:
- Communications alarm
 - Environmental alarm
 - Equipment alarm
 - Processing Error alarm
 - Software/Process alarm
 - QoS alarm
- R 20.12.** The ME-NE **SHALL** monitor, detect and generate alarm conditions and states associated with transport layer terminations (e.g., ETH PHY, SONET, etc.).
- R 20.13.** Each alarm or event notification generated by the ME-NE **SHALL** contain the following common information:
- ME-NE Identity - the unique identifier of the ME-NE generating the event notification.
 - Timestamp - the date, time, and time zone at which the event was detected by the ME-NE based on its internal system clock.
 - The failed component or list of potentially failed components. Components identified should represent the smallest replaceable/repairable units of hardware or software.
 - Probable Cause: generic trouble description
 - Specific Problems (OPTIONAL). This parameter identifies further refinements (e.g., sub-cause indicator information) to the generic trouble description of the alarm. Should also include text to provide instructions to technician.
 - Perceived Alarm Severity - Severity (i.e., critical, major, minor, warning, indeterminate, and cleared) (Severity assignments are only required for equipment alarms and physical layer communications alarms generated by the ME-NE).
 - a. Critical - Indicates that a service affecting condition has occurred and immediate corrective action is required. Such a severity is used when the managed entity is totally out of service and its capability must be restored.
 - b. Major - Indicates that a service affecting condition has occurred and urgent corrective action is required. Such a severity is used when there is a severe degradation in the capability of the managed entity and its full capability must be restored.
 - c. Minor - Indicates that a non-service affecting condition has occurred and that corrective action should be taken in order to prevent a more serious fault.

- d. Warning - Indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt.
- e. Indeterminate - Indicates that the severity level cannot be determined.
- f. Cleared - Indicates the clearing of one or more previously reported alarms.

R 20.14. In addition to the mandatory information in **R 20.13**, each alarm or event notification generated by the ME-NE **SHOULD** contain the following common information:

- Sequence Number - A unique sequence number for the reported alarm/event notification, so that the notification may be properly sequenced by the management system and such that missing or discarded notifications may be detected. **(OPTIONAL)**
- Back-up Status: This parameter indicates whether or not the entity emitting the alarm has been backed-up, and services provided to the user have, therefore, not been disrupted. A value of “true” indicates that the entity has been backed-up; a value of “false” indicates that the entity has not been backed-up. **(OPTIONAL)**
- Back-up Entity: This is the identity of the entity that is providing back-up services to the failed managed entity. **(OPTIONAL)**
- Proposed Repair Actions: This parameter, when present, is used if the cause is known and the ME-NE can suggest one or more solutions. May suggest escalation of issue. **(OPTIONAL)**
- Additional Text: This parameter is used to allow for additional text to be supplied with the alarm. Such text may further describe problem and/or failed entity (e.g., name and location). **(OPTIONAL)**

Requirements Group 21. Alarm Logging

R 21.1. The ME-NE **SHALL** log all alarms it generates; both those generated locally and those inferred from defect indications.

R 21.2. The ME-NE **SHALL** provide upon request of the managing system, the Current Problem Lists for all entities that comprise the ME-NE.

7.2 FAULT LOCALIZATION

Fault localization determines the root cause of a failure. Where the initial failure information is insufficient for fault localization it has to be augmented with information obtained by additional failure localization routines. The routines can employ internal or external test systems. Root cause analysis is performed at the EML. The ME-NE, which is present at the NEL in the TMN architecture is required to perform diagnostic operations on hardware, run checks of software and return the results to the managing system either on schedule or on request.

Requirements Group 22. Fault Diagnostics

R 22.1. The ME-NE **SHALL** on request or on schedule run diagnostics on hardware, checks on software and report the result to the managing system.

Requirements Group 23. Alarm Isolation

R 23.1. The ME-NE **SHOULD** only make a single indication of alarmed troubles.

7.3 TESTING

Testing is concerned with the testing of equipment, transport facilities and related resources within the ME-NE. Testing may be carried out for the purpose of:

- testing connecting facilities in preparation for installation of new equipment
- accepting newly installed interfaces or service assignments
- validating trouble reports
- supporting fault localization
- verification of repair.

Requirements Group 24. Diagnostic Tests

- R 24.1.** The ME-NE **SHALL** support ability to perform internal diagnostics on its internal resources.
- R 24.2.** The ME-NE **SHALL** provide diagnostics that can examine the state of each significant element of hardware, and that can identify faults and isolate failures to within the smallest replaceable unit of hardware.
- R 24.3.** The ME-NE **SHALL** permit a managing system to initiate diagnostics.

Requirements Group 25. Test Access

- R 25.1.** The ME-NE **SHOULD** provide test access to external test equipment for passively monitoring the traffic through the ME-NE interfaces. This passive monitoring shall not degrade or impact the performance of traffic.

Requirements Group 26. Fault Recovery

- R 26.1.** The ME-NE **SHOULD** allow configuration of automatic restoration and re-routing functionality (e.g., inhibited or enabled).
- R 26.2.** The ME-NE **SHOULD** support requests to force switch-to-primary. Success or failure **SHOULD** be reported.
- R 26.3.** If the standby is in operation and the primary is enabled, the ME-NE **SHOULD** support requests to manually force a switch-to-primary. Success or failure **SHOULD** be reported.
- R 26.4.** The ME-NE **SHALL** report alarms for failures that cause switch-to-protect in the same way as any other alarm.

8. Performance Management Requirements

Performance monitoring is the systematic assessment of a particular entity's ability to carry out its assigned function through the continuous collection and analysis of appropriate performance data. This section describes the functionality needed at the Network Element in support of the MEF Performance Monitoring Specification.

8.1 GENERAL PERFORMANCE MONITORING REQUIREMENTS

Requirements Group 27. Performance and Traffic Counters

- R 27.1.** Each counter used to store performance measurements **SHOULD** be capable of storing a value of at least $2^{64} - 1$.
- R 27.2.** For interval counters, in the event that an interval counter reaches its maximum value, the counter **SHALL** remain at its maximum value for the duration of the interval. These counter values **SHALL** be readable.
- R 27.3.** For continuous counters, in the event that a continuous counter reaches its maximum value, the counter **SHALL** wrap around (i.e. restart at 1). These counter values **SHALL** be readable.
- R 27.4.** The ME-NE **SHALL** associate a time stamp with the data in each past interval counter. This time stamp **SHALL** identify the time at the end of the collection interval.
- R 27.5.** All counters **SHALL** be re-settable to zero upon request. Prior to counter reset the ME-NE **SHOULD** log the value of the counter.
- R 27.6.** If events - such as failures, testing routines, or reconfigurations of an interface - occur, the ME-NE **SHALL** flag the collected data as “suspect”.
- R 27.7.** For UNI Anomalies Performance Data Set counters, UNI Traffic Performance Data Set counters, Ingress Traffic Management Performance Data Set counters, Egress Traffic Management Performance Data Set counters, and Congestion Discards Performance Data Set counters, the ME-NE **SHALL** store at least 8 hours worth of 15-minute data; the current 15-minute interval plus the past 32 15-minute intervals.
- R 27.8.** The start of every four 15-minute periods **SHOULD** be aligned with the hour boundary.

Requirements Group 28. Performance and Traffic Reporting

- R 28.1.** The ME-NE upon receiving a request from a managing system, **SHALL** provide the parameter's current or past history interval counter values as indicated on the request.
- R 28.2.** The ME-NE **SHALL** provide capabilities to produce scheduled delivery of sets of performance parameter counter values.

Requirements Group 29. Thresholded Counters

- R 29.1.** The ME-NE **SHOULD** send a Threshold Crossing Alert (TCA) to notify a managing system when a thresholded counter exceeds its threshold during a (current) measurement interval. The TCA **SHALL** contain the following information:
- a. Specific entity involved
 - b. Measurement type (e.g., FCS and Alignment Errors)
 - c. Value of the parameter
 - d. Date and time of occurrence of the event
- R 29.2.** The ME-NE **SHOULD** be capable of assigning specific threshold values to thresholded counters. Threshold values **SHALL** range from 1 to the maximum counter value.
- R 29.3.** The ME-NE **SHOULD** be capable of resetting the threshold values to a specified default.
- R 29.4.** The ME-NE **SHOULD** allow the threshold values to be modified by a managing system.
- R 29.5.** The ME-NE **SHOULD** send Threshold Crossing Alerts to the managing system within 60 seconds of the occurrence of the threshold crossing (e.g., a counter exceeding the threshold value). A maximum of one notification is sent by the ME-NE per thresholded counter during a measurement interval (e.g., the 15 minute collection period). The counter continues incrementing after the TCA has been sent.

Requirements Group 30. Performance Management Data Collection Control

- R 30.1.** The ME-NE **SHALL** provide the capability to enable/disable PM data collection functionality for the entire ME-NE, on a per performance data parameter type basis, and on a per monitored entity basis.
- R 30.2.** The ME-NE **SHALL** allow a set of performance parameter counters to be defined, specifying the parameter counters to be included in the data set and the duration of the schedule interval to be configurable.
- R 30.3.** The ME-NE **SHALL** notify managing systems when a performance data set become available for retrieval.
- R 30.4.** The ME-NE **SHALL** allow managing systems to retrieve performance data sets.

8.2 MEF SPECIFIC PERFORMANCE MONITORING REQUIREMENTS**Requirements Group 31. UNI Traffic Data Performance Data Sets**

- R 31.1.** The ME-NE **SHALL** count and **OPTIONALLY** threshold UNI Anomalies performance measurements on a per UNI basis. The **UNI Anomalies Performance Data Set SHALL** include:
- Undersized Frames
 - Oversized Frames
 - Fragments
 - Frames with FCS or Alignment Errors
 - Frames with Invalid CE-VLAN ID

R 31.2. The ME-NE **SHALL** count traffic measurements on a per UNI basis. This **UNI Traffic Performance Data Set** measurements **SHALL** include:

- Octets Transmitted OK
- Unicast Frames Transmitted OK
- Multicast Frames Transmitted OK
- Broadcast Frames Transmitted OK
- Octets Received OK
- Unicast Frames Received OK
- Multicast Frames Received OK
- Broadcast Frames Received OK

Requirements Group 32. Traffic Management Entity Performance Data Counters

R 32.1. The ME-NE **SHALL** count performance measurements on a per entity (per UNI, per COS per UNI, per EVC, or per COS per EVC) basis for each entity that enforces traffic management at Ingress direction (CE to MEN). This **Ingress Traffic Management Performance Data Set** **SHALL** include:

- `ingressGreenFrameCount`: The amount of green frames sent by the ingress UNI to the MEN
- `ingressYellowFrameCount` (**OPTIONAL**): The amount of yellow frames sent by the ingress UNI to the MEN
- `ingressRedFrameCount` (**OPTIONAL**): The amount of red (discarded) frames at the ingress UNI
- `ingressGreenOctetCount`: The amount of green octets sent by the ingress UNI to the MEN
- `ingressYellowOctetCount` (**OPTIONAL**): The amount of yellow octets sent by the ingress UNI to the MEN
- `ingressRedOctetCount` (**OPTIONAL**): The amount of red (discarded) octets at the ingress UNI

R 32.2. The ME-NE **SHALL** count performance measurements on a per entity (per UNI, per COS per UNI, per EVC, or per COS per EVC) basis for each entity that enforces traffic management at Egress direction (MEN to CE). This **Egress Traffic Management Performance Data Set** **SHALL** include:

- `egressGreenFrameCount`: The amount of green frames received by the egress UNI from the MEN
- `egressYellowFrameCount` (**OPTIONAL**): The amount of yellow frames received by the egress UNI from the MEN
- `egressGreenOctetCount`: The amount of green octets received by the egress UNI from the MEN
- `egressYellowOctetCount` (**OPTIONAL**): The amount of yellow octets received by the egress UNI from the MEN

R 32.3. The ME-NE **SHALL** count performance measurements on a per congestible resource (e.g., per UNI, per COS per UNI, per EVC, or per COS per EVC) basis in both the ingress and egress direction. This **Congestion Discards Performance Data Set** **SHALL** include:

- `greenFrameDiscards`: The amount of green frames discarded due to congestion

- yellowFrameDiscards (**OPTIONAL**): The amount of yellow frames discarded due to congestion
- greenOctetDiscards: The amount of green octets discarded due to congestion
- yellowOctetDiscards (**OPTIONAL**): The amount of yellow octets discarded due to congestion

Requirements Group 33. MAU Transport Termination Performance Monitoring

- R 33.1.** For each Transport Layer Port that represents the underlying transport termination of the Ethernet Medium Attachment Unit, the ME-NE **SHALL** count the following **MAU Termination Performance Data Set** for each MAU Transport Termination:
- Number of time the MAU leaves the *available* state (based on RFC 3636 [1] ifMauMediaAvailableStateExits)
 - Number of times the MAU enters the *jabbering* state (based on RFC 3636 [1] ifMauJabberingStateEnters)
 - Number of false carrier events during idle (based on RFC 3636 [1] ifMauFalseCarriers)

9. Security Management Requirements

Security management supports the prevention and detection of improper use of network resources and services, for the containment of and recovery from theft of services or other breaches of security, and for security administration. It includes broad categories traditionally known as Prevention, Detection, Containment and Recovery, and Security Administration. Security Management provides functions that support the enforcement of security policies to the telecommunications network and management network.

9.1 NE SECURITY MANAGEMENT REQUIREMENTS

Requirements Group 34. Identification

- R 34.1.** In support of identification of users, for all ports that accept operations-related command inputs, the ME-NE **SHALL**:
- a. Require users to identify themselves with their unique user-IDs and Password before performing any actions
 - b. Reject requests to allow an existing user-ID to be created for another user
 - c. Internally maintain the identity of all currently active users (i.e., users currently logged on)
 - d. Have the capability to disable a user-ID after a specified time interval (e.g., 90 days), if that user-ID has never been used during that time interval.
 - e. Support at least 6 character user-ID lengths
 - f. Have the capability to log-off (or lock) a user-ID after a specified time interval of inactivity (e.g., 15 minutes)

Requirements Group 35. Authentication

- R 35.1.** In support of authentication of users, for all ports that accept operations-related command inputs, the ME-NE **SHALL**:
- a. Authenticate the claimed identity of a user before allowing initial access. When the user establishes a session for the first time, the ME-NE **SHALL** prompt the user to change the password and deny the session if the user does not comply.
 - b. Not support any way to bypass the authentication mechanism.
 - c. Protect all internal storage of authentication data to ensure confidentiality.
 - d. Store passwords in a one-way encrypted form. It shall not store or retain any clear text password in any location.
 - e. Not make available to any user, passwords in clear text.
 - f. Not provide a mechanism whereby a single stored password entry can be shared by multiple user-IDs.
 - g. Provide a mechanism for a password to be user changeable.
 - h. Enforce password aging (i.e., a password is required to be changed after a specified time interval).
- R 35.2.** A user-entered password **SHOULD** contain a combination of at least six alphanumeric characters, including at least one alphabetic, one numeric, and one special (e.g., punctuation) character.
- R 35.3.** If the ME-NE can accept remote operations-related commands via public or private networks, it **SHOULD** not grant a user such access unless the user is authenticated in any of the following ways, beyond password confirmation:
- a. One time passwords, beyond reusable passwords.
 - b. Third party authentication.
 - c. Public/private key technology.

Requirements Group 36. Session Control

This requirement group describes control for a session, which begins once a user is authenticated and ends when the session is terminated (either by the user logging out or the through time-out). During a session, a user may perform authorized functions on the ME-NE.

- R 36.1.** In support of session control, for all ports that accept operations-related command inputs, the ME-NE **SHALL**:
- a. Not allow access to any user unless identified and authenticated. All ports that accept operations-related command inputs shall exercise session control.
 - b. Upon receiving erroneous authentication information, the ME-NE **SHALL** only respond that the attempt was "invalid"; i.e., it shall not reveal which part of the user-entered information (user ID and/or authenticator) is incorrect.
 - c. If the user-entered information is incorrect N times in succession, the ME-NE **SHALL** exit the login procedure and terminate the attempted session. It shall then lock out the channel (i.e., no login process can be restarted on the same port) for a specified interval of time. The lock-out time shall be configurable.
 - d. Notify the appropriate administrator via Authentication Failure Alarm when the threshold for incorrect user-entered information is exceeded.
 - e. Log the unsuccessful attempts in a special log file possibly encryption protected.
 - f. After a successful login, but before system access is granted, the ME-NE **SHALL** provide an advisory warning message regarding unauthorized entry/use and its possible consequences.

- g. Provide a mechanism for user-initiated session locking. Unlocking a locked session shall require authentication (e.g., entering the password).
- h. Provide a time-out feature. If during a session, there is no user activity for a specified amount of time, it shall lock-out the channel or require user re-authentication before accepting subsequent commands.
- i. Drop a port immediately if a session is interrupted by a power failure, link disconnection, or time-out.

Requirements Group 37. Resource Access Control

- R 37.1.** In support of resource access control, the ME-NE **SHALL**:
- a. Control access to ME-NE resources on a basis of privileges assigned to each User-Id.
 - b. Grant access rights to a single user or group of users.
 - c. Deny access rights to a single user or group of users.
 - d. Grant access rights to a single channel/port or a group of channels/ports.
 - e. Deny access rights to a single channel/port or a group of channels/ports.
- R 37.2.** The ME-NE **SHALL** allow only the authorized administrator of a resource to modify the access rights associated with the resource.

Requirements Group 38. Security Administration

- R 38.1.** The ME-NE **SHALL** support administrator functions as separate from other user functions. All users other than the appropriate administrator shall be denied permission to these administrative functions.
- R 38.2.** The ME-NE **SHALL** provide a mechanism for an appropriate administrator to:
- a. Display all users currently logged on.
 - b. Selectively audit the actions of a specified User ID.
 - c. Authorize or revoke users.
 - d. Identify all resources accessible to any specific user (and to any specific channel, where applicable) along with the associated privileges required to access them.
 - e. Create or modify a User account along with all its attributes including initial password
 - f. Create or modify a password, and delete a User-ID along with all its attributes including the password.

Requirements Group 39. Security Audit Log

- R 39.1.** The ME-NE **SHALL** generate a security log that contains information to support (post-mortem) after-the-fact investigation of loss or impropriety and appropriate management response as well as unsuccessful login attempts.
- R 39.2.** The security log **SHALL** be protected from unauthorized access or destruction. The ME-NE **SHALL** not provide any mechanism for any user, including an appropriate administrator, to modify or delete a security log.
- R 39.3.** The security log, by default, **SHALL** at least record invalid user authentication attempts, and unauthorized attempts for resource access.

- R 39.4.** For each recorded event (e.g., invalid authentication, unauthorized resource access, etc.), the security log **SHOULD** at least record the corresponding user-ID, channel/port, date, time, and information as to whether the attempt was successful.
- R 39.5.** Actual or attempted passwords **SHALL NOT** be recorded in the security log.
- R 39.6.** The ME-NE **SHOULD** allow an authorized administrator to upload post-collection audit information.

10. References

Reference	Reference Details
[1] RFC 3636	IETF RFC 3636, J. Flick, <i>Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)</i> , September 2003.
[2] MEF 10	MEF 10, <i>Ethernet Services Attributes, Phase I</i> , November 2004.
[3] MEF 7	MEF 7, <i>EMS-NMS Information Model</i> , October 2004.