CableLabs®
Access Network Independent

Network Interface Device Specification

CL-SP-NID-I01-161129

ISSUED

DISCLAIMER

This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein. Any use or reliance on the information or opinion in this document is at the risk of the user, and CableLabs and its members shall not be liable for any damage or injury incurred by any person arising out of the completeness, accuracy, or utility of any information or opinion contained in the document.

CableLabs reserves the right to revise this document for any reason including, but not limited to, changes in laws, regulations, or standards promulgated by various entities, technology advances, or changes in equipment design, manufacturing techniques, or operating procedures described, or referred to, herein.

This document is not to be construed to suggest that any company modify or change any of its products or procedures, nor does this document represent a commitment by CableLabs or any of its members to purchase any product whether or not it meets the characteristics described in the document. Unless granted in a separate written agreement from CableLabs, nothing contained herein shall be construed to confer any license or right to any intellectual property. This document is not to be construed as an endorsement of any product or company or as the adoption or promulgation of any guidelines, standards, or recommendations.

Document Status Sheet

Document Control Number:	CL-SP-NID-I01-161129			
Document Title:	Network Interface Device Specification			
Revision History:	I01 – 11/29/16			
Date:	November 29, 2016			
Status:	~~Work in Progress~~	~~Draft~~	**Issued**	~~Closed~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ Member/ Vendor~~	**Public**

Key to Document Status Codes

Work in Progress	An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.
Issued	A generally public document that has undergone Member and Technology Supplier review, cross-vendor interoperability, and is for Certification testing if applicable. Issued Specifications are subject to the Engineering Change Process.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Contents

Figures

Tables

This page intentionally left blank.

1 SCOPE

1.1 Introduction and Purpose

This specification defines an architecture and requirements for a Network Interface Device (NID) for EPON and DOCSIS® access networks and standardizes functionality satisfying service provider requirements for delivering business services. The NID specification identifies architectural elements and standardizes the method for provisioning and managing the device.

Two NID architectures are envisioned: standalone and embedded. The standalone NID is a device providing NID functionality and providing one or more local area network interfaces but no direct access network interface. The embedded NID is a device or group of components co-resident and within the same enclosure as a cable modem (CM) or optical network unit (ONU) and a communication link with the CM or ONU within the same enclosure. The two NID architecture options are illustrated in Figure 1. This specification defines requirements for the NID for either architecture. NID requirements are common for DOCSIS and DPoE™ access networks.

In the embedded model, the eNID is specified as an Embedded Service/Application Functional Entity (eSAFE) device as defined in eDOCSIS that is implemented in conjunction with an embedded DOCSIS CM or DPoE ONU.

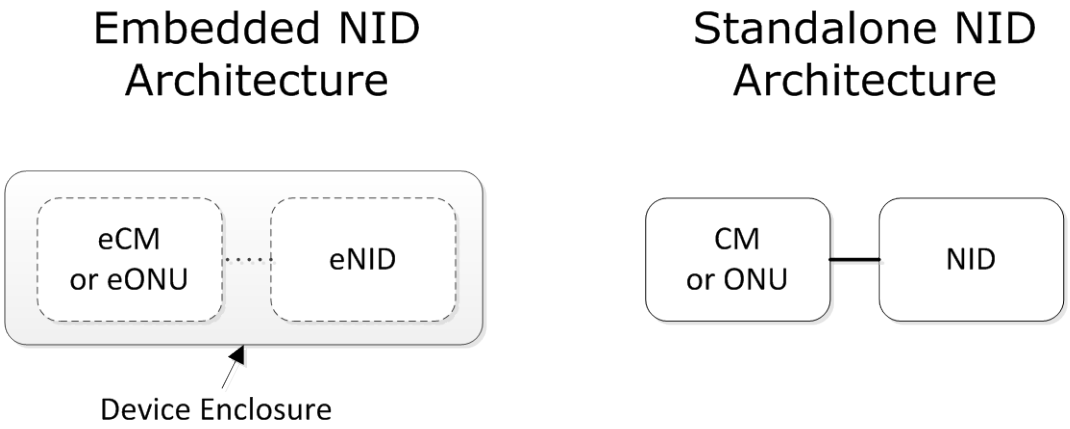

Figure 1 - Embedded NID and Standalone NID Architectures

1.2 Requirements

Throughout this document, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

2 REFERENCES

2.1 Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

All references are subject to revision, and parties to agreement based on this specification are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

[802.1ad] IEEE 802.1ad, Amendment to IEEE 802.1Q, IEEE Standard for Local and metropolitan area networks—Virtual Bridged Local Area Networks, 2006.

[802.1AX] IEEE 802.1AX, IEEE Standard for Local and metropolitan area networks--Link Aggregation, 2008.

[802.1Q] IEEE Std 802.1Q, IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Bridges and Virtual Local Area Networks, August 2011.

[802.3] IEEE Std 802.3-2015 - IEEE Standard for Ethernet, September 2015.

[ANI DEV MIB] CableLabs Access Network Independent Device MIB, CLAB-ANI-DEV-MIB, http://www.cablelabs.com/MIBs/common/.

[ANI NID MIB] CableLabs ANI Network Interface Device MIB, CLAB-ANI-NID-MIB, http://www.cablelabs.com/MIBs/common/.

[CANN DHCP] CableLabs DHCP Options Registry, CL-SP-CANN-DHCP-I13-160317, March 17, 2016, Cable Television Laboratories, Inc.

[G.8275.1] ITU-T Recommendation G.8275.1/Y.1369.1 (07/2014), Precision time protocol telecom profile for phase/time synchronization with full timing support from the network.

[IEEE 1588-2008] IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, July 24, 2008.

[L2VPN] CableLabs Layer 2 Virtual Private Networks specification, CM-SP-L2VPN-I15-150528, May 28, 2015, Cable Television Laboratories, Inc.

[MEF 6.2] MEF Technical Specification 6.2: EVC Ethernet Services Definitions Phase 3, April 2014.

[MEF 7.1] MEF Technical Specification 7.1: Phase 2 EMS-NMS Information Model, October 2009.

[MEF 10.3] MEF Technical Specification 10.3: Ethernet Services Attributes Phase 3, October 2013.

[MEF 13] MEF Technical Specification 13: User Network Interface (UNI) Type 1 Implementation Agreement, November 2005.

[MEF 17] MEF Technical Specification 17: Service OAM Requirements & Framework – Phase 1, April 2007.

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

[MEF 23.1] MEF Implementation Agreement 23.1: Carrier Ethernet Class of Service Phase 2, January 2012.

[MEF 26] MEF Technical Specification 26: External Network Network Interface (ENNI) Phase 1, January 2010.

[MEF 26.1] MEF Technical Specification 26.1: External Network Network Interface (ENNI) – Phase 2, January 2012.

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

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

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

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

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

[MEF 45] MEF Technical Specification 45: Multi-CEN L2CP, August 2014.

[MEF 46] MEF Technical Specification 46.0: Latching Loopback Protocol and Functionality, July 2014.

[MEF 49] MEF Technical Specification 49: Service Activation Testing Control Protocol and PDU Formats, October 2014.

[MULPIv3.1] DOCSIS 3.1, MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.1-I09-160602, June 2, 2016, Cable Television Laboratories, Inc.

[Q.840] ITU-T Recommendation Q.840.1 (03/2007), Requirements and analysis for NMS-EMS management interface of Ethernet over Transport and Metro Ethernet Network (EoT/MEN).

[RFC 854] IETF RFC 854, Telnet Protocol Specification, May 1983.

[RFC 950] IETF RFC 950, Internet Standard Subnetting Procedure, August 1985.

[RFC 1157] IETF RFC 1157, Simple Network Management Protocol (SNMP), May 1990.

[RFC 1213] IETF RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, March 1991.

[RFC 1350] IETF RFC 1350, The TFTP Protocol (Revision 2), July 1992.

[RFC 1492] IETF RFC 1492, An Access Control Protocol, Sometimes Called TACACS, July 1993.

[RFC 2131] IETF RFC 2131, Dynamic Host Configuration Protocol, March 1997.

[RFC 2132] IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions, March 1997.

[RFC 2544] IETF RFC 2544, Benchmarking Methodology for Network Interconnect Devices, March 1999.

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

[RFC 2710] IETF RFC 2710, Multicast Listener Discovery (MLD) for IPv6, October 1999.

[RFC 2865] IETF RFC 2865, Remote Authentication Dial In User Service (RADIUS), June 2000.

[RFC 3315] IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003.

[RFC 3410] IETF RFC 3410, Introduction and Applicability Statements for Internet-Standard Management Framework, December 2002.

[RFC 3411] IETF RFC 3411/STD0062, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, December 2002.

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

[RFC 3413] IETF RFC 3413/STD0062, Simple Network Management Protocol (SNMP) Applications, December 2002.

[RFC 3414] IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.

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

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

[RFC 3584] IETF RFC 3584, Coexistence between Version 1, Version 2 and Version 3 of the Internet-standard Network Management Framework, August 2003.

[RFC 3635] IETF RFC 3635, Definitions of Managed Objects for the Ethernet-like Interface Types, September 2003.

[RFC 4014] IETF RFC 4014, Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option, February 2005.

[RFC 4217] IETF RFC 4217, Securing FTP with TLS, October 2005.

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

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

[RFC 5357] IETF RFC 5357, A Two-Way Active Measurement Protocol (TWAMP), October 2008.

[RFC 5424] IETF RFC 5424, The Syslog Protocol, March 2009.

[RFC 5905] IETF RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010.

[Y.1564] ITU-T Recommendation Y.1564 (03/11), Ethernet service activation test methodology.

[Y.1731] ITU-T Recommendation Y.1731 (11/13), OAM functions and mechanisms for Ethernet based networks.

2.2 Informative References

This specification uses no informative references.

2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027;
  Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com
- Institute of Electrical and Electronics Engineers (IEEE), +1 800 422 4633 (USA and Canada);
  http://www.ieee.org
- ITU: International Telecommunications Union (ITU), http://www.itu.int/home/contact/index.html

- Internet Engineering Task Force (IETF) Secretariat, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, http://www.ietf.org
- MEF: Metro Ethernet Forum, 6033 W. Century Blvd, Suite 830, Los Angeles, CA 90045 Phone +1-310-642-2800; Fax +1-310-642-2808. Internet: http://metroethernetforum.org
- SCTE - Society of Cable Telecommunications Engineers Inc., 140 Philips Road, Exton, PA 19341; Phone: +1-610-363-6888 / 800-542-5040; Fax: +1-610-363-5898; http://www.scte.org/

3 TERMS AND DEFINITIONS

This specification uses the following terms:

Management Interface	The physical or logical communication interface through which the NID receives and sends SOAM messages.
Reset	Describes a routine in which the operational state is interrupted by the instruction to shut down and restart. The term is synonymous with the terms re-initialization and reboot.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

ASI	Access Side Interface
BSoD	Business Services over DOCSIS
CBS	Committed Burst Size
CCM	Continuity Check Message
CIR	Committed Information Rate
CLI	Command Line Interface
CM	Cable Modem
CMCI	Cable Modem to Customer premises equipment (CPE) Interface
CoS	Class of Service
DAD	Duplicate Address Detection
DEI	Drop Eligibility Indicator
DHCP	Dynamic Host Configuration Protocol
DMM	Delay Measurement Message
DMR	Delay Measurement Reply
DOCSIS	Data-Over-Cable Service Interface Specifications
DPoE	DOCSIS Provisioning of EPON
DTP	DOCSIS Time Protocol
EBS	Excess Burst Size
EFM	Ethernet in the First Mile
EIR	Excess Information Rate
eSAFE	Embedded Service/Application Functional Entity
EVC	Ethernet Virtual Circuit
FCAPS	Fault, Configuration, Accounting, Performance and Security
FTPS or S-FTP	FTP with TLS
GPS	Global Positioning System
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunication Union
L2CP	Layer 2 Control Protocol
LBM	Loopback Message
LBR	Loopback Reply
LTE-A	Long-term Evolution - Advanced
LTM	Linktrace Message
LTR	Linktrace Reply
MA	Maintenance Association
MEP ID	Maintenance Association End Point Identifier
MIP	Maintenance domain Intermediate Point

MSO	Multiple Systems Operator
MTU	Maximum Transmission Unit
NID	Network Interface Device
NMI	NID-to-Metro Ethernet Network (MEN) Interface
NSI	Network Side Interface
OAM	Operations, Administration, and Maintenance
ONU	Optical Network Unit
OVC	Operator Virtual Circuit
PDU	Protocol Data Unit
PM	Performance Management
PON	Passive Optical Network
PTP	Precision Time Protocol
QinQ	Also known as provider bridging, stacked VLANs per 802.1ad extension to 802.1Q
RDI	Remote Defect Indication
SAT	Service Activation Testing
SLM	Synthetic Loss Message
SLR	Synthetic Loss Reply
SNMP	Simple Network Management Protocol
SOAM	Service Operations, Administration, and Maintenance
SSH	Secure Shell
TLS	Transport Layer Security
TLV	Type-Length-Value
TWAMP	Two-Way Active Measurement Protocol
UNI	User Network Interface
VLAN	Virtual Local Area Network

5 OVERVIEW

5.1 Functional Overview

The role of the Network Interface Device (NID) is to provide the demarcation and interface between a service provider's network and the service provider's customer's network for the purpose of enabling connectivity services and other commercial services for the customer. Key roles of the NID are listed below:

- Selectively forward traffic between the service provider's network and the customer's network
- Filter packets
- Prioritize traffic
- Monitor connectivity
- Measure traffic performance
- Test service activation

5.2 Technical Overview

5.2.1 Architectural Overview

The majority of MSOs have reported that they are deploying Business Services over either DOCSIS (with or without BSoD) or PON with a CPE box solution at the customer site. The first piece of equipment as shown in the diagram is either a CM or ONU that connects to the DOCSIS or PON network as well as interconnecting another CPE device that provides Carrier Ethernet Services as shown in Figure 2 below.

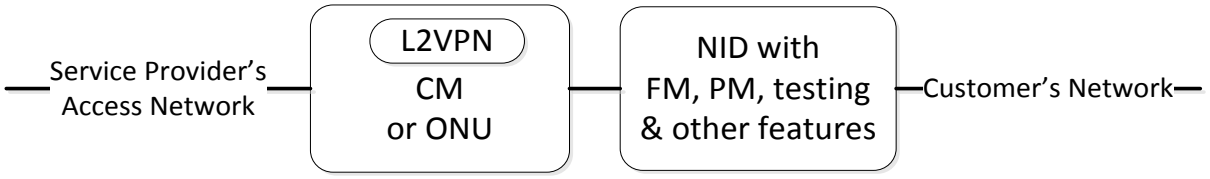

Figure 2 - Typical Business Services Deployment Scenario

Since service providers may deploy business service over different access networks, e.g., DOCSIS or PON, the NID is access network independent. It is required to work with both types of cable operator access networks and potentially others as well.

5.2.2 Protocols

The NID MUST support SNMPv2c in SNMP-coexistence mode as defined in [RFC 3584].

The NID MAY support SNMPv3 as defined in [RFC 3410], [RFC 3411], [RFC 3412], [RFC 3413], [RFC 3414], [RFC 3415] and [RFC 3584].

The NID MUST implement a mechanism for remotely configuring public and private SNMP community strings. The method for configuring SNMP agent functionality in the NID is outside the scope of this specification.

The NID MUST implement FTP secured with TLS as defined in [RFC 4217]. This is also referred to as FTPS and S-FTP.

The NID MAY support Telnet as defined in [RFC 854].

If the NID supports Telnet, the NID MUST provide a mechanism to disable Telnet through the management interface. The mechanism to disable Telnet is allowed to be vendor-specific.

The NID MUST support the Syslog protocol as defined in [RFC 5424].

If the NID implements TFTP, it MUST support TFTP version 2 as defined in [RFC 1350].

If the NID supports TFTP, the NID MUST provide a mechanism to disable TFTP through the management interface.

5.2.3 Information Models

The approach for organizing the data required by the NID is based on object-oriented modeling well-known in the industry for capturing requirements and analyzing the data in a protocol-independent representation. This approach defines requirements with use cases to describe the interactions between the operations support systems and the network element. The management information is represented in terms of objects along with their attributes and the interactions between these encapsulated objects (or also referred to as entities in some representations). The diagrams developed to capture these managed objects and their attributes and associations are UML Class Diagrams. The collection of UML Class Diagrams and Use Case Diagrams are referred to as the NID Information Models. As new NID features are added in the future and as service providers require a more proactive and efficient approach to management information, information modeling methodologies offer the ability to reuse the same definitions when new protocols are introduced in the future.

The managed objects are then represented in a protocol-specific form referred to as a management data model. The management data models when using SNMP are described using the Structure of Management Information Version 2 (SMIv2) [RFC 2578] and the design of these models is determined by the capabilities of the protocol.

6 NID REQUIREMENTS

CableLabs Network Interface Device (NID) specification describes requirements for customer premises equipment providing the demarcation between the service provider's network and their commercial services customer's network. The NID allows the service provider to provide business services compliant with Metro Ethernet Forum (MEF) Carrier Ethernet service requirements. A NID compliant with this specification satisfies requirements of a User Network Interface as defined by MEF.

The NID specification is related to CableLabs L2VPN specification [L2VPN] in the sense that both are focused on enabling the delivery of business services, but where the L2VPN specification defines requirements for CableLabs-defined cable modems (CM) and cable modem termination systems (CMTS), the NID specification is independent of CM and CMTS. As defined in Section 5.2.1, a NID compliant with this specification can be implemented as a standalone device with an Ethernet interface to connect to the access device such as a cable modem or optical network unit (ONU), or as a sub-component of an embedded device sharing an enclosure with the CM or ONU.

NID requirements are divided between Functional Requirements and SOAM Requirements. Functional requirements include forwarding requirements, provisioning requirements and clock synchronization requirements. SOAM requirements include fault management requirements, configuration management requirements, account management requirements, performance management requirements and security management requirements.

6.1 Functional Requirements

6.1.1 Forwarding Requirements

The NID MUST implement at least one [802.3]-compliant interface capable of supporting 1 Gbps transmit and receive data rate on the NSI.

The NID MAY implement at least one [802.3]-compliant interface capable of supporting 10 Gbps transmit and receive data rate on the NSI.

The NID MUST implement at least one [802.3]-compliant interface capable of supporting 1 Gbps transmit and receive data rate on the ASI.

The NID MAY implement at least one [802.3]-compliant interface capable of supporting 10 Gbps transmit and receive data rate on the ASI.

The NID MUST support L2CP handling as defined in [MEF 45].

The NID MUST support VLAN tags as defined in [802.1Q].

The NID MUST implement the 802.1ad extension part of [802.1Q], also known as provider bridging, stacked VLANs and QinQ.

The NID MUST provide the UNI for all Ethernet service types defined in [MEF 6.2] and [MEF 33].

The NID MUST support service-multiplexing as defined in [MEF 6.2].

The NID MUST discard frames received with an MTU larger than the configured MTU value.

The NID MUST be able to limit the number of configured CE-VLAN IDs that are allowed on a per-port basis per [802.1Q].

The NID MUST implement Class of Service (CoS) priorities 0 - 7 as defined in [802.1Q].

The NID MUST implement VLAN tagging using the Drop Eligibility Indicator (DEI) bit in the S-Tag and in the C-Tag as defined in [802.1Q].

The NID MUST support color marking as defined in [MEF 10.3]. Support for Color Mode and color awareness is optional.

The NID MUST support CE VLAN ID preservation and CE VLAN CoS preservation per [MEF 26.1].

The NID MUST support a minimum of eight (8) total Ethernet Virtual Circuits (EVCs) or eight (8) Operator Virtual Circuits (OVCs) per device as defined in [MEF 26].

The NID MUST support a minimum of 1024 MAC addresses per UNI. MAC address aging is controlled by the watchdog timer setting for the forwarding information base.

6.1.2 Provisioning Requirements

The NID MUST expose to a management system through a management interface its globally unique identifier formatted as a MAC address.

The NID MUST implement DHCPv4 [RFC 2131] and DHCPv6 [RFC 3315] for in-band and out-of-band interfaces.

The NID MUST support DHCPv4 options 12, 34, 60, and 61 as defined in [RFC 2132].

The NID MUST support DHCPv4 option 43 as defined in [CANN DHCP].

The NID MUST support DHCPv4 Option 82 sub-option 7 as defined in [RFC 4014].

The NID MUST be capable of decoding DHCPv4 option 34 to obtain a SYSLOG server address from the option.

The NID MUST be capable of decoding DHCPv4 option 82 sub-option 7 to obtain a RADIUS server address from the sub-option.

The NID MUST send a DHCPv6 Solicit message as described in [RFC 3315].

The NID MUST include the following information in the DHCPv6 Solicit message:

A Client Identifier option containing the DUID (DHCP Unique Identifier) for this NID as specified by [RFC 3315]. The NID can choose any one of the rules to construct the DUID according to section 9.1 of [RFC 3315];

An IA_NA (Identity Association for Non-temporary Addresses) option to obtain its IPv6 management address;

A Vendor Class option containing 32-bit number 4491 (the Cable Television Laboratories, Inc. enterprise number) and the string "CableLabs NID Specification";

A vendor-specific option containing:

1. Device ID option containing the MAC address of the HFC interface of the NID;
2. ORO option requesting the following vendor-specific options:
    a. Time Protocol Servers
    b. Time Offset
    c. TFTP Server Addresses
    d. Configuration File Name
    e. SYSLOG Server Addresses
    f. SNMP Community String

A Rapid Commit option indicating that the NID is willing to perform a 2-message DHCPv6 message exchange with the server.

The NID MUST use the following values for retransmission of the Solicit message (see [RFC 3315] for details):

- IRT (Initial Retransmission Time) = SOL_TIMEOUT
- MRT (Maximum Retransmission Time) = SOL_MAX_RT
- MRC (Maximum Retransmission Count) = 4
- MRD (Maximum Retransmission Duration) = 0

The NID MUST use the values for retransmission of the Request message defined in [RFC 3315].

If the number of DHCPv6 Solicit message retransmissions is exhausted before the NID receives an Advertise or Reply message from a DHCP server, the NID MUST consider IPv6 address acquisition to have failed.

The NID MUST support the Reconfigure Key Authentication Protocol as described in [RFC 3315]. The DHCPv6 server might be configured to use a 2-message Rapid Commit sequence. The DHCP server and NID follow [RFC 3315] in the optional use of the Rapid Commit message exchange.

The DHCPv6 server responds to Solicit and Request messages with Advertise and Reply messages (depending on the use of Rapid Commit). The Advertise and Reply messages may include other configuration parameters, as requested by the NID or as configured by the administrator to be sent to the NID. If any of the following options is absent from the DHCPv6 Advertise message, the NID MUST discard the message and wait for other Advertise messages. If any of the following options is absent from the Reply message, the NID MUST consider IPv6 address acquisition to have failed:

The IA_NA option received from the NID, containing the IPv6 management address for the NID.

A Vendor-specific Information option containing the following sub-options (refer to [CANN DHCP]):

1. Time Protocol Servers option
2. Time Offset option
3. TFTP Server Addresses option
4. Configuration File Name option
5. Syslog Server Addresses option
6. SNMP Community String

The NID MUST join the IPv6 all-nodes multicast address for its management interface and the solicited-node multicast address of the IPv6 address acquired through DHCPv6 [RFC 4862].

When joining the solicited-node multicast address of the IPv6 address acquired through DHCPv6, the NID MUST immediately report this address in an unsolicited MLD Report. The NID does not report the all-nodes multicast address [RFC 2710].

The NID MUST perform a Duplicate Address Detection with the IPv6 address acquired through DHCPv6.

If the NID determines through DAD the IPv6 address assigned through DHCPv6 is already in use by another device, the NID MUST send a DHCP Decline message to the DHCP server indicating that it has detected that a duplicate IP address exists on the link.

The NID MUST NOT continue using an IPv6 address it determines through DAD is already in use by another device.

If the NID detects that the IPv6 address it was assigned by the DHCP server is already in use, the NID MUST log an error and consider the IPv6 address acquisition to have failed.

6.1.3 Clock Synchronization Support Requirements

Certain NID applications require the ability for the NID to deliver a precise clock to subtending devices. To support these applications, this specification includes, as an optional feature, support for the Telecommunications Profile of the Precision Time Protocol as described in Annex C.

The NID MAY support network clock synchronization as defined in Annex C.

6.2 SOAM Requirements

NID Service Operations, Administration, and Maintenance (SOAM) requirements are organized below using the FCAPS ISO Telecommunications Management Network model and framework for network management.

6.2.1 Fault Management Requirements

The NID MUST Support IEEE 802.3ah link layer Ethernet-in-the-First-Mile (EFM) OAM functions including discovery, link monitoring, loopback, and fault indications between the NID and CM or ONU only.

The NID MUST receive and correctly process configuration for operation as a MEP as defined by [Y.1731].

When configured to operate as a MEP, the NID MUST correctly perform MEP functions as defined by [Y.1731].

The NID MAY receive and correctly process configuration for operation as a MIP as defined in [Y.1731].

If the NID implements MIP functionality and is configured to operate as a MIP, the NID MUST correctly perform MIP functions defined in [Y.1731].

The NID MUST implement SOAM fault management requirements defined in [MEF 30.1] for the following fault management protocols and provide a mechanism to configure them via the management interface:

- MEG ID or MAID Name
- Continuity check (CCM, RDI)
- Loopback (LBM/LBR)
- Linktrace (LTM/LTR)

The following SOAM fault management protocols defined in [MEF 30.1] are optional for the NID:

- Alarm Indicator Signal (AIS)
- Locked signal
- Test
- Client signal fail

The NID MUST support Loopback (LBM/LBR), continuity check (CCM, RDI), and Linktrace (LTM/ LTR) as defined by [MEF 46] per Maintenance Association. More than one Maintenance Association can be configured per EVC and EVCs can either be port-based or service multiplexed at a UNI.

The NID MUST support the ability to create MEPs on a per EVC basis and create MAs with different far-end MEPs.

The NID MUST implement CCM, LTM, and LBM probes as defined in [MEF 30.1] and provide a mechanism via the management interface to configure the probe interval to minimum of once per second. A one-second probe is typically employed for retail Ethernet services, and probe intervals shorter than 1 second are often used for carrier Ethernet services.

The NID MUST support the ability to generate Y.1731 messages on all EVCs concurrently at the configured probe interval.

The NID MUST implement the means to remotely initiate Loop Back testing via SNMP and command line interface (CLI).

The NID MAY implement the means to remotely initiate Loop Back testing via an out-of-band communication protocol other than SNMP and CLI.

The NID MUST implement Latching Loopback defined in [MEF 46].

The NID MUST implement SAT Test Protocol Data Units (PDU) and SAT Control PDUs defined in [MEF 49] for on-demand testing.

The NID MUST implement Session-Reflector capability of Two-Way Active Measurement Protocol (TWAMP) defined in [RFC 5357].

The NID SHOULD implement Session-Sender capability of TWAMP defined in [RFC 5357].

6.2.2 Configuration Management Requirements

This section primarily focuses on device configuration and EVC configuration, which includes configuration of EVC service attributes.

The NID receives its initiation configuration through a combination of MIB object default values and DHCP options. Remaining configuration can be accomplished through the management interface.

The NID MAY implement a TFTP client as defined in [RFC 1350].

The NID MAY be capable of receiving and decoding a file comprised of configuration settings formatted in Type-Length-Value (TLV) format.

If the NID uses a configuration file with configuration parameters encoded as TLV, the NID MUST be capable of receiving, decoding and correctly processing at least the TLV encodings listed in Annex D.

If the NID uses a configuration file with configuration parameters encoded as TLV, the NID MUST set all TLV Length fields to be greater than zero.

If the NID uses a configuration file with configuration parameters encoded as TLV, when processing a configuration file the NID MUST ignore a parameter type it does not recognize, skip over the unrecognized parameter and not treat the event as an error condition.

If the NID uses a configuration file with configuration parameters encoded as TLV, the NID MUST reject a configuration file if a TLV includes repeated sub-TLVs other than sub-TLV 53.2.

If the NID uses a configuration file with configuration parameters encoded as TLV, the NID MUST reject the configuration file if the TLV has an invalid length, or if any of the sub-TLVs have an invalid length or value.

The NID SHOULD be capable of receiving and decoding configuration settings in text-based YANG modules.

The NID MUST implement the three Classes of Service defined in [MEF 23.1].

The NID MUST support a minimum of three classes of service on EVC per UNI basis [MEF 10.3].

The NID MUST implement configurable Ingress Bandwidth Profile per UNI Service Attribute as defined in [MEF 10.3].

The NID MUST implement configurable Egress Bandwidth Profile per UNI Service Attribute as defined in [MEF 10.3].

The NID MUST implement configurable Ingress Bandwidth Profile per EVC Service Attribute as defined in [MEF 10.3].

The NID MUST implement configurable Ingress Bandwidth Profile per Class of Service Identifier Service Attribute as defined in [MEF 10.3].

The NID MUST implement configurable Egress Bandwidth Profile per EVC Service Attribute as defined in [MEF 10.3].

The NID MUST implement configurable Ingress Bandwidth Profile at the UNI as defined in [MEF 10.3].

The NID MUST implement configurable Egress Bandwidth Profile at the UNI as defined in [MEF 10.3].

The NID MUST be capable of reducing traffic burstiness at egress to the EVC per UNI, also known as traffic shaping, through configuration of CIR, CBS, EIR and EBS as described in [MEF 10.3].

The NID MUST be capable of limiting the service frame transmit rate at ingress to the EVC per UNI, also known as traffic policing, through configuration of CIR, CBS, EIR, and EBS.

The NID MUST support minimum CIR and EIR bandwidth granularity of 1 Mbps increments up to the maximum supported bandwidth of the interface.

The NID MUST provide a mechanism to configure the MTU size between 1522 octets and 2000 octets.

The NID MUST provide a Command Line Interface (CLI), web-based Graphical User Interface (GUI), or both for configuration and status monitoring.

The NID MUST NOT allow access to the operating system through the Command Line Interface.

The NID MUST provide a mechanism to remotely restrict access to the management interface to a specified set of source IP addresses (Access Control List).

The NID MUST support NTPv4 [RFC 5905], with the ability to restrict communication with only trusted NTP services.

The NID MUST provide a mechanism enabling static configuration of IP address, subnet mask, default gateway and DNS server.

The NID MUST store the current running configuration and be capable of storing one or more alternative configurations.

The NID MUST implement a mechanism to select through the management interface the configuration to be used by the device if restarted.

The NID MUST retain all configuration parameter values across device reboots.

6.2.3 Accounting Management Requirements

The NID MUST support an administrative level of access that allows creation, modification and deletion of lower-level accounts including default user accounts.

The NID MUST support hierarchy- or level-based account management, allowing for the creation of multiple levels of access. For example, administrative, user, and read-only levels of access.

The NID MUST support read only and read/write account types.

The NID MUST support a mechanism for remotely authenticating users.

The NID MUST support a mechanism for logging user access and device configuration changes for each session.

6.2.4 Performance Management Requirements

The NID MUST support Performance Monitoring Solution-1 as defined in [MEF 35] and the bins defined to count periods of unavailability.

The NID MUST support PDU types DMM/DMR, and SLM/SLR per Maintenance Association (MA) as defined in [MEF 30.1].

The NID SHOULD add hardware timestamps to DMM and DMR frames.

The NID MUST implement SNMPv2 notifications as defined in [RFC 3418].

The NID MUST implement MIBs and MIB objects listed as mandatory in Annex A.

The NID MUST provide throughput, frame delay, frame delay variation, and frame loss performance sufficient to pass Service Performance Test as defined in [Y.1564].

The NID SHOULD provide throughput, frame delay, frame delay variation, and frame loss performance sufficient to enable and satisfy benchmark testing as defined in [RFC 2544].

The NID MUST implement the means to measure and report via the management interface throughput per port and per VLAN.

The NID MUST measure and report via the management interface throughput as data offered by the customer on the UNI, accepted with transmission on the DOCSIS network interface, and delivered from the DOCSIS network interface to the Ethernet UNI.

The NID MUST measure and report via the management interface throughput as transmit and receive byte counters per service flow, where the service flow carries service frames between an ordered pair of EVC endpoints, as defined by MEF.

The NID MUST be able to test the following frame sizes: 64, 128, 256, 512, 1024, 1500 and 2000-byte frames.

The NID MUST support both IPv4 and IPv6 addressing of the management interface.

The NID MUST support all valid IP subnet masks [RFC 950] for management access.

The NID MUST maintain information for circuit and asset inventory accessible via the management interface including the information listed below:

- Location: could be latitude/longitude, physical address, asset location number, building, rack & bay (string)
- System name (string) and Z-TID
- Management IP address
- Management MAC address

- Device type, e.g., Vendor make/model or part number (string)
- Serial number
- Software version and revision
- Customer interface identifier
- Service or circuit identifier
- Target Identifier (TID)

The NID MUST support in-band and out-of-band management access, where in-band management is via configurable VLAN (mgmt-vlan) and where out-of-band management is via a physical management interface on the NID.

The NID MUST maintain configuration and circuit and asset inventory across resets.

The NID MUST implement a mechanism to record in a non-volatile event log the events listed in Annex B and as configured when event logging is enabled.

The NID MUST be capable of creating and maintaining an event log up to 2^31 – 1 bytes in size.

The NID MUST implement a mechanism for configuring the size of the event log through the management interface.

The NID MUST include a record of the date and time of occurrence with each event logged.

The NID MUST include the event description with each event logged.

The NID MUST implement a mechanism through the management interface for enabling and disabling the logging of events.

The NID MUST implement a mechanism through the management interface for starting and pausing the logging of events.

The NID MUST implement a mechanism through the management interface for clearing all entries from the event log.

The NID MUST implement a mechanism through the management interface for returning event logging settings to factory-default values.

The NID MUST be capable of logging events with multiple levels of severity as defined in Annex B.

The NID MUST implement a mechanism through the management interface for setting one or more event security levels to be logged.

The NID MUST only log events with the severity level(s) the NID is configured to log.

The NID MUST implement a mechanism through the management interface to configure severity level of each event listed in Annex B.

The NID MUST log events listed in Annex B when event logging is enabled and when it detects the event's occurrence.

When event logging is enabled and the event log buffer is full, the NID MUST record all events it is configured to record.

When event logging is enabled, the event log buffer is full and an event occurs the NID is required to add to the log, the NID MUST remove the oldest existing log entry or entries as needed to create space for the new log entry.

6.2.5 Security Management Requirements

The NID MUST support password authentication via TACACS [RFC 1492] with privilege control.

The NID MUST support password authentication via RADIUS [RFC 2865] with privilege control.

The NID MUST implement the Secure Shell (SSH) connection protocol [RFC 4254] when configured for IPv4, IPv6 or both.

The NID MUST support the ability to disable IP source-route (if applicable).

The NID MAY implement Unicast Reverse Path Forwarding (uRPF), and/or anti-spoof Access Control List (ACL), to prevent spoofing of source IP address.

6.3 MEF Compliance Requirements

The NID MUST be MEF CE 2.0 certified.

The NID MUST comply with [MEF 20].

Annex A Detailed MIB Implementation Requirements (Normative)

This Annex defines the SNMP MIB modules and MIB variables required for NID compliant with this specification.

Table 1 - MIB Implementation Support

Requirement Type	Table Notation	Description
Deprecated	D	Deprecated objects are optional. If a vendor chooses to implement the object, the object must be implemented correctly according to the MIB definition. If a vendor chooses not to implement the object, an agent must not instantiate such object and must respond with the appropriate error/exception condition (e.g., 'noSuchObject' for SNMPv2c).
Mandatory	M	The object must be implemented correctly according to the MIB definition.
Not Applicable	NA	Not applicable to the device.
Not Supported	N-Sup	An agent must not instantiate such object and must respond with the appropriate error/exception condition (e.g., 'noSuchObject' for SNMPv2c).
Optional	O	A vendor can choose to implement or not implement the object. If a vendor chooses to implement the object, the object must be implemented correctly according to the MIB definition. If a vendor chooses not to implement the object, an agent must not instantiate such object and must respond with the appropriate error/exception condition (e.g., 'noSuchObject' for SNMPv2c).
Obsolete	Ob	In SNMP convention, obsolete objects should not be implemented. This specification allows vendors to implement or not implement obsolete objects. If a vendor chooses to implement an obsoleted object, the object must be implemented correctly according to the MIB definition. If a vendor chooses not to implement the obsoleted object, the SNMP agent must not instantiate such object and must respond with the appropriate error/exception condition (e.g., 'noSuchObject' for SNMPv2c).

Table 2 - SNMP Access Requirements

SNMP Access Type	Table Notation	Description
N-Acc	Not Accessible	The object is not accessible and is usually an index in a table
Read Create	RC	The access of the object must be implemented as Read-Create
Read Write	RW	The access of the object must be implemented as Read-Write
Read Only	RO	The access of the object must be implemented as Read-Only
Read Create or Read Only	RC/RO	The access of the object must be implemented as either Read-Create or Read-Only as described in the MIB definition
Read Write / Read Only	RW/RO	The access of the object must be implemented as either Read-Write or Read-Only as described in the MIB definition
Accessible for SNMP Notifications	Acc-FN	These objects are used for SNMP Notifications by the CM SNMP Agent

A.1 MIB-Object Details

The NID instantiates SNMP MIB objects based on its configuration and operational parameters acquired during registration.

The NID is required to implement MIB objects listed as mandatory (M) in Table 3.

Table 3 - Required MIB Objects

Object	M/O	Access
MEF-SOAM-FM-MIB [MEF 31]		
mefSoamNetCfgTable	M	N-Acc
mefSoamNetCfgEntry	M	N-Acc
mefSoamNetCfgY1731Compliant	M	RC

Object	M/O	Access
mefSoamNetCfgMegIdFormat	M	RC
mefSoamNetCfgMegLevel	M	RC
mefSoamMegCfgTable	M	N-Acc
mefSoamMegCfgEntry	M	N-Acc
mefSoamMegCfgConnectivityStatusInterval	M	RC
mefSoamMegCfgPeerMepInfoAgingTime	M	RC
mefSoamMegCfgPortStatusTlvIncluded	M	RC
mefSoamMegCfgInterfaceStatusTlvIncluded	M	RC
mefSoamMepStatusTable	M	N-Acc
mefSoamMepStatusEntry	M	N-Acc
mefSoamMepStatusOperationalState	M	RO
mefSoamMepStatusConnectivityStatus	M	RO
mefSoamMepStatusSentPortStatus	M	RO
mefSoamMepStatusSentInterfaceStatus	M	RO
mefSoamMepStatusLastDefectSentStatus	M	RO
mefSoamMepStatusRdiTransmitStatus	M	RO
mefSoamMepFmStatsTable	M	N-Acc
mefSoamMepFmStatsEntry	M	N-Acc
mefSoamMepFmStatsInOamFramesDiscarded	O	RO
mefSoamMepFmStatsInCcmTotal	O	RO
mefSoamCcCfgTable	M	N-Acc
mefSoamCcCfgEntry	M	N-Acc
mefSoamCcCfgDropEligible	M	RC
mefSoamAisCfgTable	M	N-Acc
mefSoamAisCfgEntry	M	N-Acc
mefSoamAisCfgEnabled	M	RC
mefSoamAisCfgInterval	M	RC
mefSoamAisCfgPriority	M	RC
mefSoamAisCfgMdLevel	M	RC
mefSoamAisCfgDropEligible	M	RC
mefSoamAisStatsTable	M	N-Acc
mefSoamAisStatsEntry	M	N-Acc
mefSoamAisStatsOutStatus	M	RO
mefSoamAisStatsOutCounter	M	RO
mefSoamAisStatsInStatus	M	RO
mefSoamAisStatsInCounter	M	RO
mefSoamAisStatsInMacAddr	M	RO
mefSoamLbCfgTable	M	N-Acc
mefSoamLbCfgEntry	M	N-Acc
mefSoamLbCfgMulticastEnabled	M	RC
mefSoamLbCfgInterval	M	RC
mefSoamLbCfgFrameSize	M	RC
mefSoamLbCfgDataPattern	M	RC
mefSoamLbCfgTestTlvIncluded	O	RC
mefSoamLbCfgTestTlvPattern	O	RC
mefSoamLbCfgTimeout	O	RC

Object	M/O	Access
mefSoamLbStatsTable	M	N-Acc
mefSoamLbStatsEntry	M	N-Acc
mefSoamLbStatsNumLbrInCrcErrors	M	RO
mefSoamLbrMulticastTable	O	N-Acc
mefSoamLbrMulticastEntry	O	N-Acc
mefSoamLbrMulticastTransId	O	N-Acc
mefSoamLbrMulticastReceiveOrder	O	N-Acc
mefSoamLbrMulticastReplyMac	O	RO
mefSoamLtStatsTable	M	N-Acc
mefSoamLtStatsEntry	M	N-Acc
mefSoamLtLtmTransmitted	M	RO
mefSoamLtLtrReceived	M	RO
mefSoamLtLtmReceived	O	RO
mefSoamLtLtrTransmitted	O	RO
mefSoamLckCfgTable	O	N-Acc
mefSoamLckCfgEntry	O	N-Acc
mefSoamLckCfgAdminState	O	RC
mefSoamLckCfgInterval	O	RC
mefSoamLckCfgPriority	O	RC
mefSoamLckCfgMdLevel	O	RC
mefSoamLckStatsTable	O	N-Acc
mefSoamLckStatsEntry	O	N-Acc
mefSoamLckStatsInStatus	O	RO
mefSoamLckStatsInCounter	O	RO
mefSoamLckStatsOutStatus	O	RO
mefSoamLckStatsOutCounter	O	RO
mefSoamTestCfgTable	M	N-Acc
mefSoamTestCfgEntry	M	N-Acc
mefSoamTestCfgOutEnabled	O	RC
mefSoamTestCfgInEnabled	O	RC
mefSoamTestCfgInService	O	RC
mefSoamTestCfgDestMacAddress	O	RC
mefSoamTestCfgDestMepId	O	RC
mefSoamTestCfgDestIsMepId	O	RC
mefSoamTestCfgInterval	O	RC
mefSoamTestCfgPriority	O	RC
mefSoamTestCfgDropEligible	O	RC
mefSoamTestCfgFrameSize	O	RC
mefSoamTestCfgPattern	O	RC
mefSoamTestCfgStartTimeType	O	RC
mefSoamTestCfgScheduledStartDateAndTime	O	RC
mefSoamTestCfgScheduledStopDateAndTime	O	RC
mefSoamTestCfgRelativeStartTime	O	RC
mefSoamTestCfgDurationTime	O	RC
mefSoamTestCfgOutStatus	O	RC
mefSoamTestStatsTable	O	N-Acc

Object	M/O	Access
mefSoamTestStatsEntry	O	N-Acc
mefSoamTestStatsNumIn	O	RO
mefSoamTestStatsNumInOutOfOrder	O	RO
mefSoamTestStatsNumInCrcErrors	O	RO
mefSoamTestStatsNumInBerErrors	O	RO
mefSoamTestStatsNumOut	O	RO
Fault Management Notifications		
mefSoamAlarmInterval	O	RW
mefSoamAlarmEnable	O	RW
Notifications (Traps)		
mefSoamMepDefectAlarm	M	
mefSoamConfigErrorAssertAlarm	M	
mefSoamConfigErrorClearAlarm	M	
mefSoamMepOperStatusAlarm	M	
mefSoamLckAlarm	O	
mefSoamAisAlarm	O	
MEF-SOAM-PM-MIB [MEF 36]		
mefSoamPmMepTable	M	N-Acc
mefSoamPmMepEntry	M	N-Acc
mefSoamPmMepOperNextIndex	M	RO
mefSoamPmMepLmSingleEndedResponder	O	RW
mefSoamPmMepSlmSingleEndedResponder	M	RW
mefSoamPmMepDmSingleEndedResponder	M	RW
mefSoamLmCfgTable	M	N-Acc
mefSoamLmCfgEntry	M	N-Acc
mefSoamLmCfgIndex	M	N-Acc
mefSoamLmCfgType	M	RC
mefSoamLmCfgVersion	O	RC
mefSoamLmCfgEnabled	M	RC
mefSoamLmCfgMeasurementEnable	M	RC
mefSoamLmCfgMessagePeriod	M	RC
mefSoamLmCfgPriority	M	RC
mefSoamLmCfgFrameSize	M	RC
mefSoamLmCfgDataPattern	M	RC
mefSoamLmCfgTestTlvIncluded	O	RC
mefSoamLmCfgTestTlvPattern	O	RC
mefSoamLmCfgMeasurementInterval	M	RC
mefSoamLmCfgNumIntervalsStored	M	RC
mefSoamLmCfgDestMacAddress	M	RC
mefSoamLmCfgDestMepId	M	RC
mefSoamLmCfgDestIsMepId	M	RC
mefSoamLmCfgStartTimeType	M	RC
mefSoamLmCfgFixedStartDateAndTime	M	RC
mefSoamLmCfgRelativeStartTime	M	RC
mefSoamLmCfgStopTimeType	M	RC
mefSoamLmCfgFixedStopDateAndTime	M	RC

Object	M/O	Access
mefSoamLmCfgRelativeStopTime	M	RC
mefSoamLmCfgRepetitionTime	M	RC
mefSoamLmCfgAlignMeasurementIntervals	O	RC
mefSoamLmCfgAlignMeasurementOffset	O	RC
mefSoamLmCfgAvailabilityMeasurementInterval	M	RC
mefSoamLmCfgAvailabilityNumConsecutiveMeasPdus	M	RC
mefSoamLmCfgAvailabilityFlrThreshold	M	RC
mefSoamLmCfgAvailabilityNumConsecutiveIntervals	M	RC
mefSoamLmCfgAvailabilityNumConsecutiveHighFlr	O	RC
mefSoamLmCfgSessionType	M	RC
mefSoamLmCfgSessionStatus	M	RC
mefSoamLmCfgHistoryClear	M	RC
mefSoamLmCfgRowStatus	M	RC
mefSoamLmMeasuredStatsTable	M	N-Acc
mefSoamLmMeasuredStatsEntry	M	N-Acc
mefSoamLmMeasuredStatsForwardFlr	O	RO
mefSoamLmMeasuredStatsBackwardFlr	O	RO
mefSoamLmMeasuredStatsAvailForwardStatus	O	RO
mefSoamLmMeasuredStatsAvailBackwardStatus	O	RO
mefSoamLmMeasuredStatsAvailForwardLastTransitionTime	M	RO
mefSoamLmMeasuredStatsAvailBackwardLastTransitionTime	M	RO
mefSoamLmCurrentAvailStatsTable	M	N-Acc
mefSoamLmCurrentAvailStatsEntry	M	N-Acc
dot1agCfmMdIndex,	M	N-Acc
dot1agCfmMaIndex,	M	N-Acc
dot1agCfmMepIdentifier,	M	N-Acc
mefSoamLmCfgIndex	M	N-Acc
dot1agCfmMdIndex,	M	N-Acc
dot1agCfmMaIndex,	M	N-Acc
mefSoamLmCurrentAvailStatsIndex	M	RO
mefSoamLmCurrentAvailStatsStartTime	M	RO
mefSoamLmCurrentAvailStatsElapsedTime	M	RO
mefSoamLmCurrentAvailStatsSuspect	M	RO
mefSoamLmCurrentAvailStatsForwardHighLoss	O	RO
mefSoamLmCurrentAvailStatsBackwardHighLoss	O	RO
mefSoamLmCurrentAvailStatsForwardConsecutiveHighLoss	O	RO
mefSoamLmCurrentAvailStatsBackwardConsecutiveHighLoss	O	RO
mefSoamLmCurrentAvailStatsForwardAvailable	M	RO
mefSoamLmCurrentAvailStatsBackwardAvailable	M	RO
mefSoamLmCurrentAvailStatsForwardUnavailable	M	RO
mefSoamLmCurrentAvailStatsBackwardUnavailable	M	RO
mefSoamLmCurrentAvailStatsForwardMinFlr	O	RO
mefSoamLmCurrentAvailStatsForwardMaxFlr	O	RO
mefSoamLmCurrentAvailStatsForwardAvgFlr	O	RO
mefSoamLmCurrentAvailStatsBackwardMinFlr	O	RO
mefSoamLmCurrentAvailStatsBackwardMaxFlr	O	RO

Object	M/O	Access
mefSoamLmCurrentAvailStatsBackwardAvgFlr	O	RO
mefSoamLmCurrentStatsTable	M	N-Acc
mefSoamLmCurrentStatsEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamLmCfgIndex	M	N-Acc
mefSoamLmCurrentStatsIndex	M	RO
mefSoamLmCurrentStatsStartTime	M	RO
mefSoamLmCurrentStatsElapsedTime	M	RO
mefSoamLmCurrentStatsSuspect	M	RO
mefSoamLmCurrentStatsForwardTransmittedFrames	O	RO
mefSoamLmCurrentStatsForwardReceivedFrames	O	RO
mefSoamLmCurrentStatsForwardMinFlr	O	RO
mefSoamLmCurrentStatsForwardMaxFlr	O	RO
mefSoamLmCurrentStatsForwardAvgFlr	O	RO
mefSoamLmCurrentStatsBackwardTransmittedFrames	O	RO
mefSoamLmCurrentStatsBackwardReceivedFrames	O	RO
mefSoamLmCurrentStatsBackwardMinFlr	O	RO
mefSoamLmCurrentStatsBackwardMaxFlr	O	RO
mefSoamLmCurrentStatsBackwardAvgFlr	O	RO
mefSoamLmCurrentStatsSoamPdusSent	M	RO
mefSoamLmCurrentStatsSoamPdusReceived	M	RO
mefSoamLmHistoryAvailStatsTable	M	N-Acc
mefSoamLmHistoryAvailStatsEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamLmCfgIndex	M	N-Acc
mefSoamLmHistoryAvailStatsIndex	M	N-Acc
mefSoamLmHistoryAvailStatsIndex	M	N-Acc
mefSoamLmHistoryAvailStatsEndTime	M	RO
mefSoamLmHistoryAvailStatsElapsedTime	M	RO
mefSoamLmHistoryAvailStatsSuspect	M	RO
mefSoamLmHistoryAvailStatsForwardHighLoss	O	RO
mefSoamLmHistoryAvailStatsBackwardHighLoss	O	RO
mefSoamLmHistoryAvailStatsForwardConsecutiveHighLoss	O	RO
mefSoamLmHistoryAvailStatsBackwardConsecutiveHighLoss	O	RO
mefSoamLmHistoryAvailStatsForwardAvailable	M	RO
mefSoamLmHistoryAvailStatsBackwardAvailable	M	RO
mefSoamLmHistoryAvailStatsForwardUnavailable	M	RO
mefSoamLmHistoryAvailStatsBackwardUnavailable	M	RO
mefSoamLmHistoryAvailStatsForwardMinFlr	O	RO
mefSoamLmHistoryAvailStatsForwardMaxFlr	O	RO
mefSoamLmHistoryAvailStatsForwardAvgFlr	O	RO
mefSoamLmHistoryAvailStatsBackwardMinFlr	O	RO

Object	M/O	Access
mefSoamLmHistoryAvailStatsBackwardMaxFlr	O	RO
mefSoamLmHistoryAvailStatsBackwardAvgFlr	O	RO
mefSoamLmHistoryStatsTable	M	N-Acc
mefSoamLmHistoryStatsEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamLmCfgIndex	M	N-Acc
mefSoamLmHistoryStatsIndex	M	N-Acc
mefSoamLmHistoryStatsEndTime	M	RO
mefSoamLmHistoryStatsElapsedTime	M	RO
mefSoamLmHistoryStatsSuspect	M	RO
mefSoamLmHistoryStatsForwardTransmittedFrames	O	RO
mefSoamLmHistoryStatsForwardReceivedFrames	O	RO
mefSoamLmHistoryStatsForwardMinFlr	O	RO
mefSoamLmHistoryStatsForwardMaxFlr	O	RO
mefSoamLmHistoryStatsForwardAvgFlr	O	RO
mefSoamLmHistoryStatsBackwardTransmittedFrames	O	RO
mefSoamLmHistoryStatsBackwardReceivedFrames	O	RO
mefSoamLmHistoryStatsBackwardMinFlr	O	RO
mefSoamLmHistoryStatsBackwardMaxFlr	O	RO
mefSoamLmHistoryStatsBackwardAvgFlr	O	RO
mefSoamLmHistoryStatsSoamPdusSent	M	RO
mefSoamLmHistoryStatsSoamPdusReceived	M	RO
mefSoamDmCfgTable	M	N-Acc
mefSoamDmCfgEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamDmCfgIndex	M	N-Acc
mefSoamDmCfgType	M	RC
mefSoamDmCfgVersion	O	RC
mefSoamDmCfgEnabled	M	RC
mefSoamDmCfgMeasurementEnable	M	RC
mefSoamDmCfgMessagePeriod	M	RC
mefSoamDmCfgPriority	M	RC
mefSoamDmCfgFrameSize	M	RC
mefSoamDmCfgDataPattern MefSoamTcDataPatternType,	M	RC
mefSoamDmCfgTestTlvIncluded	O	RC
mefSoamDmCfgTestTlvPattern	O	RC
mefSoamDmCfgMeasurementInterval	M	RC
mefSoamDmCfgNumIntervalsStored	M	RC
mefSoamDmCfgDestMacAddress	M	RC
mefSoamDmCfgDestMepId	M	RC
mefSoamDmCfgDestIsMepId	M	RC
mefSoamDmCfgSourceMacAddress	O	RC

Object	M/O	Access
mefSoamDmCfgStartTimeType	M	RC
mefSoamDmCfgFixedStartDateAndTime	M	RC
mefSoamDmCfgRelativeStartTime	M	RC
mefSoamDmCfgStopTimeType MefSoam	M	RC
mefSoamDmCfgFixedStopDateAndTime	M	RC
mefSoamDmCfgRelativeStopTime	M	RC
mefSoamDmCfgRepetitionTime	M	RC
mefSoamDmCfgAlignMeasurementIntervals	M	RC
mefSoamDmCfgAlignMeasurementOffset	O	RC
mefSoamDmCfgNumMeasBinsPerFrameDelayInterval	M	RC
mefSoamDmCfgNumMeasBinsPerInterFrameDelayVariationInterval	M	RC
mefSoamDmCfgInterFrameDelayVariationSelectionOffset	O	RC
mefSoamDmCfgNumMeasBinsPerFrameDelayRangeInterval	M	RC
mefSoamDmCfgSessionType	M	RC
mefSoamDmCfgSessionStatus	M	RC
mefSoamDmCfgHistoryClear	M	RC
mefSoamDmCfgRowStatus RowStatus	M	RC
mefSoamDmCfgMeasBinTable	M	N-Acc
mefSoamDmCfgMeasBinEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamDmCfgIndex	M	N-Acc
mefSoamDmCfgMeasBinType	M	N-Acc
mefSoamDmCfgMeasBinNumber	M	N-Acc
mefSoamDmCfgMeasBinType	M	N-Acc
mefSoamDmCfgMeasBinNumber	M	N-Acc
mefSoamDmCfgMeasBinLowerBound	M	RW
mefSoamDmMeasuredStatsTable	M	N-Acc
mefSoamDmMeasuredStatsEntry	M	N-Acc
mefSoamDmMeasuredStatsFrameDelayTwoWay	O	RO
mefSoamDmMeasuredStatsFrameDelayForward	O	RO
mefSoamDmMeasuredStatsFrameDelayBackward	O	RO
mefSoamDmMeasuredStatsIfdvTwoWay	O	RO
mefSoamDmMeasuredStatsIfdvForward	O	RO
mefSoamDmMeasuredStatsIfdvBackward	O	RO
mefSoamDmCurrentStatsTable	M	N-Acc
mefSoamDmCurrentStatsEntry	M	N-Acc
mefSoamDmCurrentStatsIndex	M	N-Acc
mefSoamDmCurrentStatsStartTime	M	RO
mefSoamDmCurrentStatsElapsedTime	M	RO
mefSoamDmCurrentStatsSuspect	M	RO
mefSoamDmCurrentStatsFrameDelayTwoWayMin	M	RO
mefSoamDmCurrentStatsFrameDelayTwoWayMax	M	RO
mefSoamDmCurrentStatsFrameDelayTwoWayAvg	M	RO
mefSoamDmCurrentStatsFrameDelayForwardMin	M	RO

Object	M/O	Access
mefSoamDmCurrentStatsFrameDelayForwardMax	M	RO
mefSoamDmCurrentStatsFrameDelayForwardAvg	M	RO
mefSoamDmCurrentStatsFrameDelayBackwardMin	M	RO
mefSoamDmCurrentStatsFrameDelayBackwardMax	M	RO
mefSoamDmCurrentStatsFrameDelayBackwardAvg	M	RO
mefSoamDmCurrentStatsIfdvForwardMin	M	RO
mefSoamDmCurrentStatsIfdvForwardMax	M	RO
mefSoamDmCurrentStatsIfdvForwardAvg	M	RO
mefSoamDmCurrentStatsIfdvBackwardMin	M	RO
mefSoamDmCurrentStatsIfdvBackwardMax	M	RO
mefSoamDmCurrentStatsIfdvBackwardAvg	M	RO
mefSoamDmCurrentStatsIfdvTwoWayMin	O	RO
mefSoamDmCurrentStatsIfdvTwoWayMax	O	RO
mefSoamDmCurrentStatsIfdvTwoWayAvg	O	RO
mefSoamDmCurrentStatsFrameDelayRangeForwardMax	M	RO
mefSoamDmCurrentStatsFrameDelayRangeForwardAvg	M	RO
mefSoamDmCurrentStatsFrameDelayRangeBackwardMax	M	RO
mefSoamDmCurrentStatsFrameDelayRangeBackwardAvg	M	RO
mefSoamDmCurrentStatsFrameDelayRangeTwoWayMax	O	RO
mefSoamDmCurrentStatsFrameDelayRangeTwoWayAvg	O	RO
mefSoamDmCurrentStatsSoamPdusSent	M	RO
mefSoamDmCurrentStatsSoamPdusReceived	M	RO
mefSoamDmCurrentStatsBinsTable	M	N-Acc
mefSoamDmCurrentStatsBinsEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamDmCfgIndex	M	N-Acc
mefSoamDmCfgMeasBinType	M	N-Acc
mefSoamDmCfgMeasBinNumber	M	N-Acc
mefSoamDmCurrentStatsBinsCounter	M	RO
mefSoamDmHistoryStatsTable	M	N-Acc
mefSoamDmHistoryStatsEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamDmCfgIndex	M	N-Acc
mefSoamDmHistoryStatsIndex	M	N-Acc
mefSoamDmHistoryStatsEndTime	M	RO
mefSoamDmHistoryStatsElapsedTime	M	RO
mefSoamDmHistoryStatsSuspect	M	RO
mefSoamDmHistoryStatsFrameDelayTwoWayMin	M	RO
mefSoamDmHistoryStatsFrameDelayTwoWayMax	M	RO
mefSoamDmHistoryStatsFrameDelayTwoWayAvg	M	RO
mefSoamDmHistoryStatsFrameDelayForwardMin	M	RO
mefSoamDmHistoryStatsFrameDelayForwardMax	M	RO

Object	M/O	Access
mefSoamDmHistoryStatsFrameDelayForwardAvg	M	RO
mefSoamDmHistoryStatsFrameDelayBackwardMin	M	RO
mefSoamDmHistoryStatsFrameDelayBackwardMax	M	RO
mefSoamDmHistoryStatsFrameDelayBackwardAvg	M	RO
mefSoamDmHistoryStatsIfdvForwardMin	M	RO
mefSoamDmHistoryStatsIfdvForwardMax	M	RO
mefSoamDmHistoryStatsIfdvForwardAvg	M	RO
mefSoamDmHistoryStatsIfdvBackwardMin	M	RO
mefSoamDmHistoryStatsIfdvBackwardMax	M	RO
mefSoamDmHistoryStatsIfdvBackwardAvg	M	RO
mefSoamDmHistoryStatsIfdvTwoWayMin	O	RO
mefSoamDmHistoryStatsIfdvTwoWayMax	O	RO
mefSoamDmHistoryStatsIfdvTwoWayAvg	O	RO
mefSoamDmHistoryStatsFrameDelayRangeForwardMax	M	RO
mefSoamDmHistoryStatsFrameDelayRangeForwardAvg	M	RO
mefSoamDmHistoryStatsFrameDelayRangeBackwardMax	M	RO
mefSoamDmHistoryStatsFrameDelayRangeBackwardAvg	M	RO
mefSoamDmHistoryStatsFrameDelayRangeTwoWayMax	O	RO
mefSoamDmHistoryStatsFrameDelayRangeTwoWayAvg	O	RO
mefSoamDmHistoryStatsSoamPdusSent	M	RO
mefSoamDmHistoryStatsSoamPdusReceived	M	RO
mefSoamDmHistoryStatsBinsTable	M	N-Acc
mefSoamDmHistoryStatsBinsEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamDmCfgIndex	M	N-Acc
mefSoamDmHistoryStatsIndex	M	N-Acc
mefSoamDmCfgMeasBinType	M	N-Acc
mefSoamDmCfgMeasBinNumber	M	N-Acc
mefSoamDmHistoryStatsBinsCounter	M	RO
mefSoamLmThresholdCfgTable	M	N-Acc
mefSoamLmThresholdCfgEntry	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
dot1agCfmMaIndex	M	N-Acc
dot1agCfmMepIdentifier	M	N-Acc
mefSoamLmCfgIndex	M	N-Acc
mefSoamLmThresholdCfgIndex	M	N-Acc
dot1agCfmMdIndex	M	N-Acc
mefSoamLmThresholdCfgEnable	M	RC
mefSoamLmThresholdCfgMeasuredFlrForwardThreshold	O	RC
mefSoamLmThresholdCfgMaxFlrForwardThreshold	M	RC
mefSoamLmThresholdCfgAvgFlrForwardThreshold	M	RC
mefSoamLmThresholdCfgMeasuredFlrBackwardThreshold	O	RC
mefSoamLmThresholdCfgMaxFlrBackwardThreshold	M	RC
mefSoamLmThresholdCfgAvgFlrBackwardThreshold	M	RC

Object	M/O	Access
mefSoamLmThresholdCfgForwardHighLossThreshold	O	RC
mefSoamLmThresholdCfgForwardConsecutiveHighLossThreshold	O	RC
mefSoamLmThresholdCfgBackwardHighLossThreshold	O	RC
mefSoamLmThresholdCfgBackwardConsecutiveHighLossThreshold	O	RC
mefSoamLmThresholdCfgForwardUnavailCountThreshold	M	RC
mefSoamLmThresholdCfgForwardAvailRatioThreshold	M	RC
mefSoamLmThresholdCfgBackwardUnavailCountThreshold	M	RC
mefSoamLmThresholdCfgBackwardAvailRatioThreshold	M	RC
mefSoamLmThresholdCfgRowStatus	M	RC
mefSoamDmThresholdCfgTable	M	N-Acc
mefSoamDmThresholdCfgEntry	M	N-Acc
mefSoamDmThresholdCfgIndex	M	N-Acc
mefSoamDmThresholdCfgEnable	M	RC
mefSoamDmThresholdCfgMeasuredFrameDelayTwoWayThreshold	O	RC
mefSoamDmThresholdCfgMaxFrameDelayTwoWayThreshold	M	RC
mefSoamDmThresholdCfgAvgFrameDelayTwoWayThreshold	M	RC
mefSoamDmThresholdCfgMeasuredIfdvTwoWayThreshold	O	RC
mefSoamDmThresholdCfgMaxIfdvTwoWayThreshold	O	RC
mefSoamDmThresholdCfgAvgIfdvTwoWayThreshold	O	RC
mefSoamDmThresholdCfgMaxFrameDelayRangeTwoWayThreshold	O	RC
mefSoamDmThresholdCfgAvgFrameDelayRangeTwoWayThreshold	O	RC
mefSoamDmThresholdCfgMeasuredFrameDelayForwardThreshold	O	RC
mefSoamDmThresholdCfgMaxFrameDelayForwardThreshold	M	RC
mefSoamDmThresholdCfgAvgFrameDelayForwardThreshold	M	RC
mefSoamDmThresholdCfgMeasuredIfdvForwardThreshold	O	RC
mefSoamDmThresholdCfgMaxIfdvForwardThreshold	M	RC
mefSoamDmThresholdCfgAvgIfdvForwardThreshold	M	RC
mefSoamDmThresholdCfgMaxFrameDelayRangeForwardThreshold	M	RC
mefSoamDmThresholdCfgAvgFrameDelayRangeForwardThreshold	M	RC
mefSoamDmThresholdCfgMeasuredFrameDelayBackwardThreshold	O	RC
mefSoamDmThresholdCfgMaxFrameDelayBackwardThreshold	M	RC
mefSoamDmThresholdCfgAvgFrameDelayBackwardThreshold	M	RC
mefSoamDmThresholdCfgMeasuredIfdvBackwardThreshold	O	RC
mefSoamDmThresholdCfgMaxIfdvBackwardThreshold	M	RC
mefSoamDmThresholdCfgAvgIfdvBackwardThreshold	M	RC
mefSoamDmThresholdCfgMaxFrameDelayRangeBackwardThreshold	M	RC
mefSoamDmThresholdCfgAvgFrameDelayRangeBackwardThreshold	M	RC
mefSoamDmThresholdCfgRowStatus	M	RC
Performance Management Notifications		
mefSoamPmNotificationCfgAlarmInterval	M	RW
mefSoamPmNotificationCfgAlarmEnable	M	RW
mefSoamPmNotificationObjDateAndTime	M	Acc-FN
mefSoamPmNotificationObjThresholdId	O	Acc-FN
mefSoamPmNotificationObjThresholdConfig	O	Acc-FN
mefSoamPmNotificationObjThresholdValue	O	Acc-FN
mefSoamPmNotificationObjSuspect	M	Acc-FN

Object	M/O	Access
mefSoamPmNotificationObjCrossingType	O	Acc-FN
mefSoamPmNotificationObjDestinationMep	M	Acc-FN
mefSoamPmNotificationObjPriority	M	Acc-FN
Notifications (Traps)		
mefSoamAvailabilityChangeAlarm		
mefSoamLmSessionStartStopAlarm		
mefSoamDmSessionStartStopAlarm		
mefSoamPmThresholdCrossingAlarm		
EtherLike-MIB [RFC 3635]		
dot3StatsTable	M	N-Acc
dot3StatsEntry	M	N-Acc
dot3StatsIndex	M	RO
dot3StatsAlignmentErrors	M	RO
dot3StatsFCSErrors	M	RO
dot3StatsSingleCollisionFrames	M	RO
dot3StatsMultipleCollisionFrames	M	RO
dot3StatsSQETestErrors	M	RO
dot3StatsDeferredTransmissions	M	RO
dot3StatsLateCollisions	M	RO
dot3StatsExcessiveCollisions	M	RO
dot3StatsInternalMacTransmitErrors	M	RO
dot3StatsCarrierSenseErrors	M	RO
dot3StatsFrameTooLongs	M	RO
dot3StatsInternalMacReceiveErrors	M	RO
dot3StatsEtherChipSet	M	RO
dot3StatsSymbolErrors	M	RO
dot3StatsDuplexStatus	M	RO
dot3StatsRateControlAbility	M	RO
dot3StatsRateControlStatus	M	RO
dot3CollTable	M	N-Acc
dot3CollEntry	M	N-Acc
dot3CollCount	M	N-Acc
dot3CollFrequencies	M	RO
dot3ControlTable	M	N-Acc
dot3ControlEntry	M	N-Acc
dot3ControlFunctionsSupported	M	RO
dot3ControlInUnknownOpcodes	M	RO
dot3HCControlInUnknownOpcodes	M	RO
dot3PauseTable	M	N-Acc
dot3PauseEntry	M	N-Acc
dot3PauseAdminMode	M	RW
dot3PauseOperMode	M	RO
dot3InPauseFrames	M	RO
dot3OutPauseFrames	M	RO
dot3HCInPauseFrames	M	RO
dot3HCOutPauseFrames	M	RO

Object	M/O	Access
dot3HCStatsTable	M	N-Acc
dot3HCStatsEntry	M	N-Acc
dot3HCStatsAlignmentErrors	M	RO
dot3HCStatsFCSErrors	M	RO
dot3HCStatsInternalMacTransmitErrors	M	RO
dot3HCStatsFrameTooLongs	M	RO
dot3HCStatsInternalMacReceiveErrors	M	RO
dot3HCStatsSymbolErrors	M	RO
dot3HCStatsAlignmentErrors	M	RO
CLAB-ANI-DEV-MIB [ANI DEV MIB]		
aniDevResetNow	M	RW
aniDevLoggingControlReset	M	RW
aniDevSystemLoggingSize	M	RW
aniDevSystemLoggingLevelControl	M	RW
aniDevSystemLoggingGroupControl	M	RW
aniDevSystemLoggingEventTable	M	N-Acc
aniDevSystemLoggingEventEntry	M	N-Acc
aniDevSystemLoggingEventIndex	M	N-Acc
aniDevSystemLoggingEventTimeStamp	M	RO
aniDevSystemLoggingEventMessage	M	RO
RFC1213-MIB aka MIB-II [RFC 1213]		
sysObjectID	M	RO
sysUpTime	M	RO
sysContact	O	RW
sysLocation	M	RW
sysServices	M	RO
ifNumber	M	RO
ifTable	M	N-Acc
ifEntry	M	N-Acc
ifIndex	M	RO
ifDescr	M	RO
ifType	M	RO
ifMtu	M	RO
ifSpeed	M	RO
ifPhysAddress	M	RO
ifAdminStatus	M	RW
ifOperStatus	M	RO
ifLastChange	M	RO
ifInOctets	M	RO
ifInUcastPkts	M	RO
ifInNUcastPkts	M	RO
ifInDiscards	M	RO
ifInErrors	M	RO
ifInUnknownProtos	M	RO
ifOutOctets	M	RO
ifOutUcastPkts	M	RO

Object	M/O	Access
ifOutNUcastPkts	M	RO
ifOutDiscards	M	RO
ifOutErrors	M	RO
ifOutQLen	M	RO
ifSpecific	M	RO
CLAB-ANI-NID-MIB [ANI NID MIB]		
clabAniNidCfgID	M	RO
clabAniNidCfgPtpMcastMac	M	R/W
clabAniNidCfgTelnetEnabled	M	R/W
clabAniNidCfgTftpEnabled	M	R/W
clabAniNidCfgClientAuthStatus	M	RO
clabAniNidCfgAuthServerServiceType	M	RW
clabAniNidCfgPrimaryServerIpAddressType	M	RW
clabAniNidCfgPrimaryServerIpAddress	M	RW
clabAniNidCfgPrimaryServerPort	M	RW
clabAniNidCfgSecondaryServerIpAddressType	M	RW
clabAniNidCfgSecondaryServerIpAddress	M	RW
clabAniNidCfgSecondaryServerPort	M	RW
clabAniNidStatusAuthHistoryMaximumTableSize	M	RW
clabAniNidStatusAuthHistoryTable	M	NA
clabAniNidStatusAuthHistoryEntry	M	NA
clabAniNidStatusAuthInitiationTime	M	RO
clabAniNidStatusAuthResults	M	RO
clabAniNidStatusAuthServer	M	RO
clabAniNidStatusReportCircuitReportTable	M	RO
clabAniNidStatusReportCircuitEntry	M	NA
clabAniNidStatusReportCircuitIdentifier	M	RO
clabAniNidStatusReportCircuitTargetIdentifier	M	RO

Annex B Format and Content for Event, SYSLOG, and SNMP Notification (Normative)

Table 4 in this annex summarizes the format and content for event, syslog, and SNMP notifications required for a NID.

Each row specifies a possible event that may appear in the NID. These events are to be reported by a NID through local event logging, and may be accompanied by syslog or SNMP notification.

The "Process" and "Sub-Process" columns indicate in which stage the event happens. The "NID Priority" column indicates the priority the event is assigned in the NID.

The "Event Message" column specifies the event text. The "Message Notes And Details" column provides additional information about the event text in the "Event Message" column. Some of the text fields include variable information. The variables are explained in the "Message Notes And Details" column. For some events the "Message Notes And Details" column may include the keyword <Deprecated> to indicate this event is being deprecated and its implementation is optional. For events where the "Event Message" or "Message Notes and Details" column includes either <P1> or <P2>, there is a single space between the value as defined by the <P1> or <P2> and the preceding text.

This specification defines the following keywords as part of the "Event Message" column:

"<TAGS>" (without the quotes) corresponds to: <NID-MAC>;<NID-VER>"

Where:

<NID-MAC>: NID MAC Address;

Format*: "NID-MAC=xx:xx:xx:xx:xx:xx"

<NID-VER>: NID Specification Version;

Format*: "NID-VER=1.0"

(*) without the quotes

The NID MUST format the NID MAC Address field <NID-MAC> of the Event Message text using lowercase letters.

The NID MAY append additional vendor-specific text to the end of the event text.

The "Error Code Set" column specifies the error code. The "Event ID" column indicates a unique identification number for the event.

The "Notification Name" column specifies the SNMP notification, which notifies this event to an SNMP notification receiver.

Example DHCP Notification and Syslog message "Event Message" text string for Event ID 68000100:

DHCP FAILED - Discover sent, no offer received;NID-MAC=00:22:ce:03:f4:da;NID-VER=1.0;

Table 4 - Event Format and Content

Process	Sub-Process	NID Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID	Notification Name
DHCP, TOD and TFTP							
DHCP		Error	DHCP RENEW sent - No response for <P1><TAGS>	P1=IPv4 or IPv6	D101.0	68010100	
DHCP		Error	DHCP REBIND sent - No response for <P1><TAGS>	P1=IPv4 or IPv6	D102.0	68010200	
DHCP		Error	DHCP RENEW WARNING - Field invalid in response <P1> option<TAGS>	P1=v4	D103.0	68010300	
DHCP		Critical	DHCP RENEW FAILED - Critical field invalid in response		D103.1	68010301	
DHCP		Error	DHCP REBIND WARNING - Field invalid in response <TAGS>		D104.0	68010400	
DHCP		Critical	DHCP REBIND FAILED - Critical field invalid in response		D104.1	68010401	
DHCP		Notice	DHCP Reconfigure received<TAGS>		D105.0	68010500	
DHCP		Notice	DHCP Renew - lease parameters <P1> modified<TAGS>	P1 = list of params that changed at renew	D106.0	68010600	
DHCP		Error	Primary lease failed, IPv4 fallback initiated<TAGS>		D107.0	68010700	
Init	DHCP	Critical	DHCP FAILED - Discover sent, no offer received<TAGS>		D01.0	68000100	
Init	DHCP	Critical	DHCP FAILED - Request sent, No response<TAGS>		D02.0	68000200	
Init	DHCP	Warning	DHCP WARNING - Non-critical field invalid in response <TAGS>		D03.0	68000300	
Init	DHCP	Critical	DHCP FAILED - Critical field invalid in response <TAGS>		D03.1	68000301	
Init	DHCP	Critical	DHCP failed - RS sent, no RA received<TAGS>		D12.0	68001200	
Init	DHCP	Critical	DHCP Failed - Invalid RA<TAGS>		D12.1	68001201	
Init	DHCP	Critical	DHCP failed - DHCP Solicit sent, No DHCP Advertise received<TAGS>		D12.2	68001202	
Init	DHCP	Critical	DHCP failed - DHCP Request sent, No DHCP REPLY received<TAGS>		D12.3	68001203	
Init	DHCP	Error	Primary address acquired, secondary failed<TAGS>		D12.4	68001204	

Process	Sub-Process	NID Priority	Event Message	Message Notes and Detail	Error Code Set	Event ID	Notification Name
Init	DHCP	Error	Primary address failed, secondary active<TAGS>		D12.5	68001205	
Init	IPv6 Address Acquisition	Critical	Link-Local address failed DAD<TAGS>		D13.1	68001301	
Init	IPv6 Address Acquisition	Critical	DHCP lease address failed DAD<TAGS>		D13.2	68001302	
Init	TFTP	Warning	TFTP failed - Request sent - No Response<TAGS>		D05.0	68000500	
Init	TFTP	Warning	TFTP failed - configuration file NOT FOUND<TAGS>	For SYSLOG only: append: File name = <P1> P1 = requested file name	D06.0	68000600	
Init	TFTP	Warning	TFTP Failed - OUT OF ORDER packets<TAGS>		D07.0	68000700	
Init	TFTP	Warning	TFTP file complete - but failed Message Integrity check MIC<TAGS>	For SYSLOG only: append: File name = <P1> P1 = file name of TFTP file	D08.0	68000800	
Init	TFTP	Warning	TFTP file complete - but missing mandatory TLV<TAGS>		D09.0	68000900	
Init	TFTP	Warning	TFTP Failed - file too big<TAGS>		D10.0	68001000	
Init	TFTP	Warning	TFTP file complete- but doesn't enable 2.0 Mode - conflicts with current US channel type<TAGS>	For SYSLOG only: append: File name = <P1> P1 = file name of TFTP file	D11.0	68001100	
Init	TFTP	Warning	TFTP Request Retries exceeded, CM unable to register	For SYSLOG only: append: File name = <P1> P1 = file name of TFTP file	D11.1	68001101	
DHCP		Error	DHCP RENEW sent - No response for <P1><TAGS>	P1=IPv4 or IPv6	D101.0	68010100	

Annex C Clock Synchronization Requirements (Normative)

As described in Section 6.1.3, support for the clock synchronization requirements in this section is optional.

The Precision time protocol telecom profile developed by ITU provides a method for a precise clock reference to be distributed by a network. The "telecom profile" is based on the Precision Time Protocol (PTP) defined in [IEEE 1588-2008], with some modifications.

NOTE: At the time of the development of this Annex, a single version of the telecom profile has been published as [G.8275.1] that defines the use of PTP over Ethernet. It has been reported that work in the ITU on a second version has been approved and is in a pre-publication phase. It is currently referred to as G.8275.2 that is expected to define the use of PTP over IP. In the context of a NID device participating in the distribution of precise clock timing, there is a need for support both for PTP over Ethernet and for PTP over IP. There is an expectation that the PTP over IP definition in G.8275.2 will be preferable to PTP over IP as defined in [IEEE 1588-2008], but until the Recommendation is published, this cannot be confirmed. Manufacturers building NID implementations are recommended to consult with their customers regarding whether support for G.8275.2 is required.

In NID deployments where precise clock distribution is required, the NID will be expected to derive clock from the network operator (via the DOCSIS CM or DPoE ONU). DOCSIS 3.1 CMs include optional support for [G.8275.1], which is the preferred clock source when it is available. In the absence of [G.8275.1], the NID will be expected to acquire clock via PTP over IP.

The NID supporting this Annex MUST support ITU G.8275.1 on its NID-to-Metro Ethernet Network (MEN) Interface (NMI) to acquire clock from an upstream master clock. The NID supporting this Annex MUST support PTP/IP [IEEE 1588-2008] on its NMI to acquire clock from an upstream master clock.

The NID supporting this Annex MUST support a standardized method to deliver clock via its UNI to customer devices. The NID supporting this Annex MUST support ITU G.8275.1 on its UNI to provide clock to customer devices. The NID supporting this Annex MAY support PTP/IP [IEEE 1588-2008] on its UNI to provide clock to customer devices.

The NID supporting this Annex MUST support a configuration interface to allow the operator to select either the forwardable multicast address (1) or the non-forwardable multicast address (2) to use for clock distribution [G.8275.1].

At the time of writing this specification, an expected application for a NID supporting this Annex is to provide connectivity and clock for LTE-A small cell base stations. The end-to-end clock accuracy requirement for a small cell base station (relative to a common system master clock) is determined to be ±1500 ns. To achieve this level of accuracy requires the use of DOCSIS 3.1 equipment that supports the optional DOCSIS Time Protocol (DTP) feature with “Level IV” accuracy (see [MULPIv3.1]). The resulting clock distribution error budget is provided below.

Table 5 - Clock Distribution Error Budget

Clock Distribution Error Component	Budget
T-dtp-iv-error (DOCSIS CMCI compared to common master clock) (T-cm-cm-skew/2 for a Level IV DTP system)	± 750 ns
T-network1-error (NID NMI compared to DOCSIS CMCI)	± 100 ns*
T-nid-error (NID UNI compared to NMI)	± 200 ns
T-network2-error (Small Cell Network Interface compared to NID UNI)	± 100 ns*
T-small-cell-error (RF clock compared to Small Cell Network Interface)	± 350 ns
Total Small Cell RF Clock Error (RF clock compared to common master clock)	± 1500 ns

* Total of ±200ns error introduced by switches in-line between CM and Small Cell. Not all deployments will incorporate switches.

The NID supporting this Annex MUST meet the T-nid-error accuracy requirement in Table 5.

In typical deployments, the accuracy of the G.8275.1 clock that is acquired by the NID will be affected by the accuracy of the clock delivery path from the master clock to the NID. In the case of a DOCSIS 3.1 CM supporting

DTP, one significant source of inaccuracy arises due to the propagation delay asymmetry of the HFC plant. The Level IV budget in [MULPIv3.1] allows ±150 ns for the error due to this asymmetry, which may be achievable in many plants. However, this asymmetry has been measured in some cases to be more than 1800 ns, resulting in a clock error of more than 900 ns. In the case of a DPoE ONU, or the case of a DOCSIS CM that does not support DTP, there is additional inaccuracy due to forwarding and MAC layer latency differences between the upstream and downstream paths. These inaccuracies could be on the order of multiple milliseconds. In deployments that rely on the G.8275.1 clock of the NID to provide an accurate clock phase reference (such as LTE small cell devices), a means to correct for this static asymmetry is required.

The NID supporting this Annex MUST support a clock offset value that is used to correct for path asymmetry between the NID and the master clock. The NID supporting this Annex MUST correct its internal clock using this offset value when providing the clock reference to attached devices via its UNI.

The NID supporting this Annex MUST store the clock offset value in nonvolatile memory.

The NID supporting this Annex MUST support a management interface to allow the operator to set the clock offset value.

The NID supporting this Annex SHOULD support a GPS calibration feature to automatically determine the clock offset value. The NID supporting GPS calibration MUST have a GPS antenna input with an SMA connector. The operator can connect a GPS antenna temporarily to the NID, allowing the NID to calibrate its network clock. During calibration, the NID acquires its position and GPS clock. The NID supporting GPS calibration MUST compare its internal clock (acquired via the network) to the GPS clock. Upon successful acquisition of clock and position from GPS, the NID stores (in nonvolatile memory) the location, the measured clock offset, and the date and time the calibration was performed, overwriting any previous or manually configured values for those parameters. The NID supporting GPS calibration SHOULD continuously calculate the clock offset value whenever both GPS lock and the network clock are available. For future calibration operations, the NID supporting GPS calibration SHOULD use stored location to accelerate satellite acquisition. The NID supporting GPS calibration MUST make both the clock offset value and the stored location available for read and write access via the management interface. The NID supporting GPS calibration SHOULD have an indicator light that indicates successful GPS lock and calibration.

The NID MAY support a GPS master clock mode in which it operates continuously with GPS clock (permanently connected antenna) and uses the G.8275.1 clock as a backup clock for reliability (extended holdover time).

Annex D Common TLV Encodings (Normative)

Table 6 provides a summary of the top-level TLV encodings the NID is required to understand and correctly process.

Table 6 - Required TLV Encodings

Type	Description	Length	Additional Detail
0	Pad	-	
11	SNMP MIB Object	n	
53	SNMPv1v2c Coexistence	n	

D.1 Encodings for Configuration

The NID MUST be capable of decoding the following type/length/value encodings in the configuration file. All multi-octet quantities are transmitted to the NID in network-byte order, i.e., the octet containing the most-significant bits is the first transmitted on the wire.

D.1.1 SNMP MIB Object

This object allows arbitrary SNMP MIB objects to be Set via the TFTP-Registration process.

Type	Length	Value
11	N	variable binding

The value is an SNMP VarBind as defined in [RFC 1157]. The VarBind is encoded in ASN.1 Basic Encoding Rules, just as it would be if part of an SNMP Set request.

The NID MUST treat this object as if it were part of an SNMP Set Request with the following caveats:

- The request is treated as fully authorized (it cannot refuse the request for lack of privilege).
- SNMP Write-Control provisions do not apply.
- No SNMP response is generated by the NID.

This object could be repeated with different VarBinds to "Set" a number of MIB objects. The NID MUST treat all such Sets as if simultaneous.

The NID MUST reject any VarBind greater than 255 bytes long.

D.1.2 SNMPv1v2c Coexistence

This object specifies the SNMPv1v2c Coexistence Access Control configuration of the NID.

The NID MUST be capable of receiving and processing a minimum of 10 SNMPv1v2c Coexistence TLVs.

The NID MUST reject the configuration file if the configuration file contains SNMPv1v2 Coexistence Configuration encodings and if the SNMPv1v2c Community Name and SNMPv1v2c Transport Address Access sub-TLVs are not present.

The NID MUST support multiple instances of sub-TLV 53.2 SNMPv1v2c Transport Address Access.

Type	Length	Value
53	N	Composite

Annex E NID SOAM Reporting Requirements (Normative)

E.1 Overview

This Annex defines the NID Service, Operations, Administration and Maintenance (SOAM) reporting requirements.

E.1.1 NID Fault Management OAM Object Definitions

The NID is required to implement Service OAM Fault Management reporting as defined by [MEF 31]. In particular the NID is required to implement MEF-SOAM-FM-MIB defined in [MEF 31]. The MEF-SOAM-FM-MIB is based on the Fault Management Objects described in [MEF 7.1], which refers in turn to [Q.840].

E.1.2 NID Performance Management OAM Object Definitions

The NID is required to implement Service OAM Performance Management reporting as defined by [MEF 36]. In particular the NID is required to implement MEF-SOAM-PM-MIB defined in [MEF 36]. The MEF-SOAM-PM-MIB is based on SOAM Performance Monitoring functions defined in [MEF 17] and the Performance Management Function Set described in [MEF 7.1], which refers in turn to [Q.840].

Appendix I Acknowledgements

CableLabs thanks the following participants contributing directly to this document:

Contributor	Company Affiliation
Michael Waldo	Adva Optical
Ryan Kener	Comcast
Saifur Rahman	Comcast
Hesham El Bakoury	Huawei
Rajiv Papneja	Huawei
Fuad Alnajjar	Mediacom
Lance Hassan	Time Warner Cable/Charter Communications
Kirk Erichsen	Time Warner Cable/Charter Communications
Kevin Noll	Time Warner Cable/Charter Communications
Rudy Zijlstra	Vodafone
Greg White	CableLabs
Steve Burroughs	CableLabs
James Kim	CableLabs
Kevin Luehrs	CableLabs
Stuart Hoggan	CableLabs