Superseded

Cable Data Services

DOCSIS® Provisioning of EPON Specifications

DPoE™ Demarcation Device Specification

DPoE-SP-DEMARCv1.0-I01-120410

ISSUED

Notice

This DPoE specification is the result of a cooperative effort undertaken by certain member companies of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs®. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. 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

Document Status Sheet

Document Control Number:	DPoE-SP-DEMARCv1.0-I01-120410			
Document Title:	DPoE™ Demarcation Device Specification			
Revision History:	I01 – Released 04/10/12			
Date:	April 10, 2012			
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 stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Contents

Figures

Tables

1 INTRODUCTION

DOCSIS Provisioning of EPON (DPoE) specifications are a joint effort of CableLabs, cable operators, vendors, and suppliers to support EPON technology using existing DOCSIS-based back office systems and processes.

Ethernet PON or EPON is an IEEE Ethernet 802.3 standard for a passive optical network (PON). A PON is a specific type of multi-access optical network. A multi-access optical network is an optical fiber-based network technology that permits more than two network elements to transmit and receive on the same fiber. Appendix I in [DPoE-ARCHv1.0] has a more detailed explanation of multi-access optical networks.

This version of the DPoE specifications focuses on DOCSIS-based provisioning and operations of Internet Protocol (IP) using DOCSIS Internet service (which is typically referred to as High Speed Data (HSD)), or IP(HSD), and Metro Ethernet (MEF) services. DPoE Networks offer IP(HSD) services functionally equivalent to DOCSIS networks using a model similar to DOCSIS, where the DPoE System acts like a DOCSIS CMTS, and the DPoE System and DPoE ONU act like a DOCSIS CM.

1.1 DEMARC Introduction

The DEMARC was introduced in DPoE specifications to fill a need by operators for a device to act as the demarcation point between the MSO's DPoE Network access interface on the DPoE ONU (D-ONU), and the Customer Equipment (CE) as defined in the Metro Ethernet Forum MEF specifications. By definition the DEMARC is an Ethernet device connected to D-ONU MEF I-NNI (MI) interface providing one or more MEF UNI (MU) interfaces to one or more CE devices.

The DEMARC is not a Customer Premise Equipment (CPE) as defined in DOCSIS or DPoE specifications. The specifications contained herein do not apply to a device connected to the Cable Modem to CPE Interface (CMCI).

The DEMARC in one scenario may play the role of a Network Interface Device (NID). In some cases, a DPoE ONU is sufficient to meet the operator's needs. There are a variety of reasons that an operator might elect to use a DEMARC with a D-ONU rather than just a D-ONU. Among these reasons may be factors such as:

Port requirements

The wide variety of devices that can be a DEMARC includes switches, routers, NIDs, gateways, firewalls, security devices, and many other types of Ethernet devices that provide Metro Ethernet or other services. DEMARCs might be used by operators to provide a larger number or greater variety of Ethernet port types. DEMARCs might also be used by operators to provide ports for other (over the top) services as described below.

Physical Requirements

DEMARCs can have operators' requirements that extend beyond the DPoE specifications. These could, for example, include physical requirements such as those for rack-mounting, outside plant operations, electrical power, or other physical requirements.

Multiple Tenant Unit Requirements

DEMARCs are likely to be used for Multiple Tenant facilities because they have a larger number of ports. Operators may also have additional requirements for management and operations of a DEMARC that is used to provide services to multiple customers.

Over-the-Top Services

DEMARCs can also be used by operators to provide services beyond the Metro Ethernet services. For example, an operator might use a DEMARC to provide MU interfaces and also run IP(HSD) services on other ports. Another example might be MU interfaces and a "soft MU" (terminated on the DEMARC) with IP running over the Metro Ethernet service to a SIP proxy with IP/Ethernet, FXS or NxT1 interface(s) for voice.

Other Requirements

Operators might need advanced service management and Metro Ethernet circuit management features such as SOAM, QoS, over-the-top IP/MPLS (such as U-PE), or other functionality that is not provided by stand-alone D-ONUs.

1.2 Scope

This specification describes some of the requirements for DEMARCs for providing Metro Ethernet services (as described by the MEF) with a D-ONU. This specification is not a comprehensive set of requirements for a DEMARC because, by definition, the requirements for the DEMARC include physical, port, service, management, and other requirements that are beyond the scope of the DPoE specifications.

The focus of the DEMARC specification is on the requirements for the interface between the D-ONU and the DEMARC. This specification also provides a means for automating the in-band management path for the DEMARC, and for transferring a configuration file to the DEMARC.

1.3 Goals

Operators are likely to widely use DEMARCs to meet a variety of Metro Ethernet and over-the-top service needs for both single-tenant and multi-tenant businesses or commercial services. The goal of this specification is to:

- Describe, but not specify, basic requirements for MEF functionality for a DEMARC.
- Describe the use of MI and MU with a DEMARC.
- Provide detailed requirements for the automatic distribution of a pre-existing device configuration from the operator's Operations and Support Systems (OSS) to the DEMARC.
- Provide independence of automation from the type of pluggable or baseband interface on the DEMARC.

Since the MI and MU interface requirements (which the DEMARC uses) are clearly specified in [DPoE-MEFv1.0], this specification will make reference to that specification, but not provide any additional technical requirements for those interfaces. This specification is focused on a description of the DEMARC Automatic Configuration (DAC) process, which is designed to perform a similar function to DOCSIS and DPoE (CM and vCM respectively) device provisioning.

Historically, operators configured the DEMARC manually with either an Element Management System (EMS)/Network Management System (NMS) or by manually writing configuration files.

1.4 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.

1.5 DPoE Version 1.0 Specifications

A list of the specifications included in the DPoE version 1.0 series is provided in Table 1. For further information please refer to http://www.cablelabs.com/dpoe/specifications.

Table 1 - DPoE 1.0 Series of Specifications

Designation	Title
DPoE-SP-ARCHv1.0	DPoE Architecture Specification
DPoE-SP-DEMARCv1.0	DPoE Demarcation Device Specification
DPoE-SP-OAMv1.0	DPoE OAM Extensions Specification
DPoE-SP-PHYv1.0	DPoE Physical Layer Specification
DPoE-SP-SECv1.0	DPoE Security and Certificate Specification
DPoE-SP-IPNEv1.0	DPoE IP Network Element Requirements
DPoE-SP-MULPIv1.0	DPoE MAC and Upper Layer Protocols Interface Specification
DPoE-SP-MEFv1.0	DPoE Metro Ethernet Forum Specification
DPoE-SP-OSSIv1.0	DPoE Operations and Support System Interface Specification

1.6 History of the DEMARC Specification

The release timing of this DEMARC specification differs from the release of other DPoE version 1.0 specifications. The DEMARC specification was originally slated to be part of the next version of DPoE specifications, but an urgent need by cable operators to simplify the provisioning of DEMARCs for business services deployments provided motivation to release this specification sooner. Releasing this specification sooner than originally planned provides suppliers an earlier opportunity to develop products that meet an important cable operator requirement, allows operators to begin adjusting their back office systems to support DEMARCs, and it also affords CableLabs the opportunity to include this functionality during interoperability testing events.

Since the genesis of this specification was originally as part of the next version of DPoE specifications, there are terms introduced in this document that extend the concepts and terminology beyond that which was used in the other DPoE version 1.0 specifications. Generally, these terms are well defined and their meaning will be clear to readers of this specification.

1.7 Reference Architecture

The DPoE reference architecture identifies the elements that a DPoE Network minimally requires to illustrate and communicate the physical hardware and logical software interfaces between the functional subsystems of the DPoE architecture. The principal elements in the architecture are the DPoE System that resides in the operator network and the DPoE ONU, which may be an off-the-shelf EPON ONU or EPON SFP-ONU. The remaining elements in the architecture are existing servers and systems in the operator's network. All of the server elements have connectivity through an IP (TCP/IP) network. Transport of bearer traffic and (in some cases) Layer 2 (L2) OAM signaling is available through either IP or L2 Ethernet-based Network Interfaces.

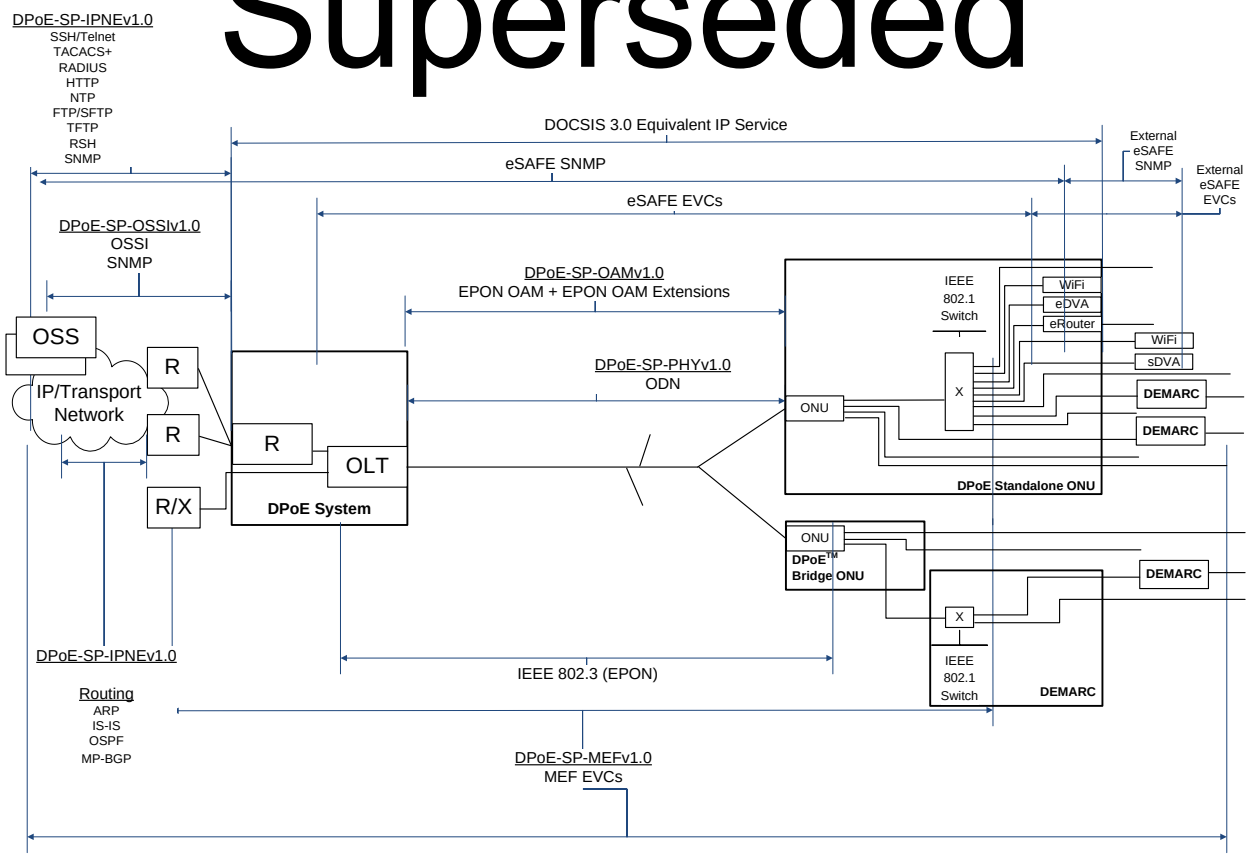

Figure 1 - DPoEv1.0 Reference Architecture

1.8 DPoE Interfaces and Reference Points

The DPoE interfaces and reference points provide a basis for the description and enumeration of DPoE specifications for the DPoE architecture. Each interface or reference point indicates a point between separate sub-systems. The reference points have protocols that run across them, or have a common format of bearer traffic (with no signaling protocol). All of the interfaces are bi-directional interfaces that support two-way communications. The protocols in DPoE specifications operate within different layers based on the [802.3], [802.1], IETF, MEF, and CableLabs specifications. The C reference points are uni-directional for upstream (C_O) or downstream (C_S) classification, respectively.

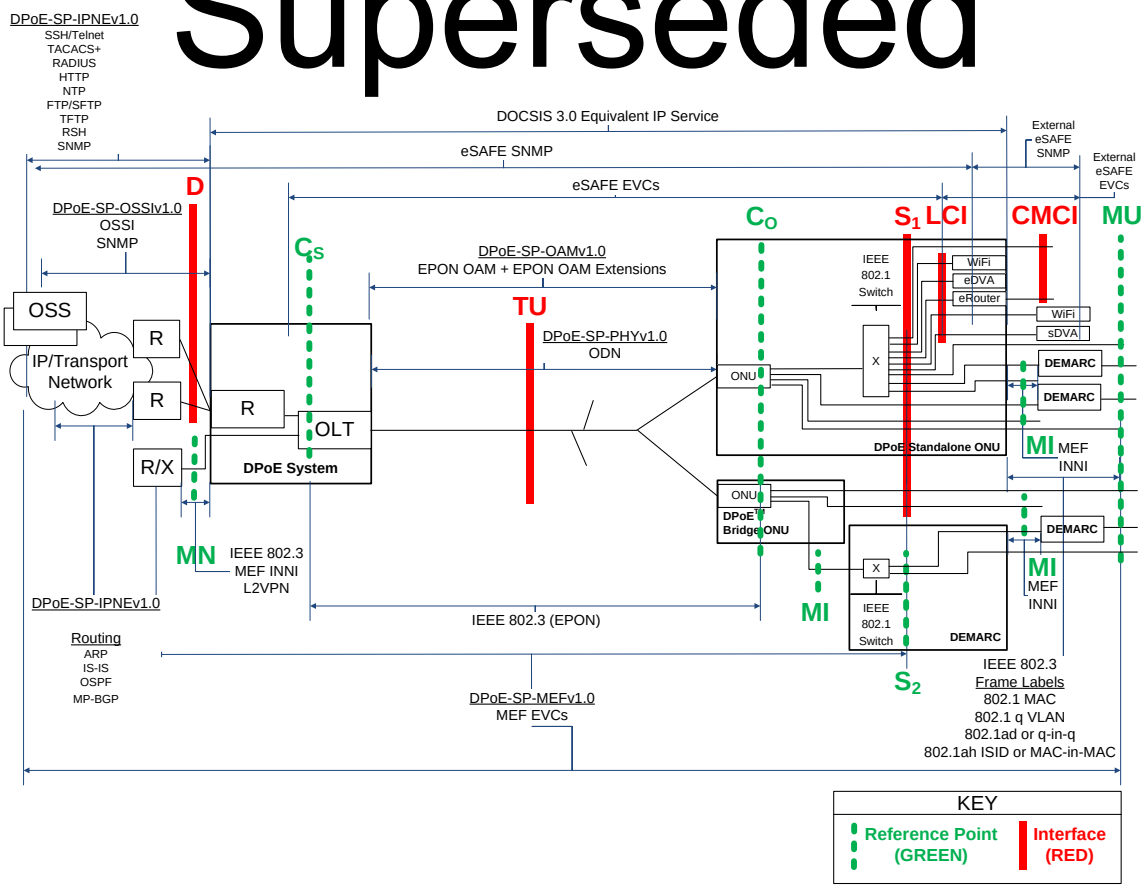

Figure 2 - DPoEv1.0 Interfaces and Reference Points

Table 2 - DPoEv1.0 Interface and Reference Point Descriptions

Interface or Reference Point		Interface or Reference Point Description
MN		The MN interface is an [802.3] interface for Ethernet (or MEF or L2VPN emulated) services only. It serves the role of a MEF INNI or L2VPN NSI. It is an NNI for Metro Ethernet services only.
D		The D interface is the DOCSIS IP NNI interface. It is an operator network facing interface, sometimes called a Network to Network Interface (NNI) or Network Systems Interface (NSI) in DOCSIS specifications. The D interface allows a DPoE System to communicate with an IP network. The D interface carries all IP management traffic including OSSI and IP NE traffic. The D interface carries all DOCSIS IP service traffic.
TU		The TU interface is a short form of expressing the interface between the DPoE System and the DPoE ONU.
C		The C reference point is used for explanation of traffic ingress to a DPoE classifier.
	C_O	The C_O reference point is used for explanation of traffic ingress to a DPoE ONU upstream classifier.
	C_S	The C_S reference point is used for explanation of traffic ingress to a DPoE System downstream classifier.
S		The S interface is an IEEE 802 interface. The S interface may be an internal interface (such as [802.3] across a GMII SERDES or XGMII interface in an SFP-ONU, SFP+ONU or XFP-ONU) or it may be an external Ethernet interface. S_1 is an interface for a DPoE Standalone ONU. S_2 is a reference point used for explanation of services with the DPoE Bridge ONU.
	S_1	The S_1 interfaces are the general case of all interfaces on a DPoE Standalone ONU. S_1 interfaces may be CMCI, LCI, MI, or MU interfaces.
	S_2	The S_2 reference point is used for explanation of traffic ingress to and egress from interfaces on a DEMARC device in a DPoE System. Although there are no specifications or requirements for the S_2 reference point, informative text refers to the S_2 reference point to provide the full context for the use of a DPoE Bridge ONU in a DEMARC device providing Metro Ethernet services.
LCI		The Logical CPE Interface (LCI) interface is an eDOCSIS interface as defined in [eDOCSIS]. The eDOCSIS architecture is [802.1d] MAC-based according to the DOCSIS 3.0 specifications; however, DOCSIS L2VPN clearly supports [802.1Q] switching. In practice, therefore, the eDOCSIS interface consists of a DOCSIS classifier and [802.1] switch as illustrated. The function of a DOCSIS classifier is in part replaced by forwarding (tagging and encapsulation) in MEF and in part covered by classifiers in this specification.
CMCI		CMCI is the DPoE interface equivalent of the DOCSIS Cable Modem CPE Interface as defined in [CMCIv3.0]. This is the service interface for DOCSIS-based IP services.
MI		MI is usually an S interface (or S reference point) that operates as a MEF INNI. A DPoE ONU that provides a MEF INNI has an MI interface. A DPoE ONU can have MU as an interface and an MI reference point on different S interfaces in a single DPoE ONU. The MI interface or reference point is an [802.3] interface (or reference point) between a DPoE ONU and a DEMARC device.

Interface or Reference Point	Interface or Reference Point Description
MU	MU is usually an S interface (or S reference point) that operates as a MEF UNI. A DPoE ONU that directly provides a MEF UNI (MU) interface has MU as an interface. A DPoE ONU can have MU as an interface and an MI reference point on different S interfaces in a single DPoE ONU. The MU interface or reference point is an [802.3] interface (or reference point) between a DPoE ONU or a DEMARC device and a customer's equipment.

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. At the time of publication, the editions indicated were valid. All references are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below. References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific. For a non-specific reference, the latest version applies.

In this specification, terms "802.1ad" and "802.1ah" are used to indicate compliance with the [802.1ad] and [802.1ah] standards, respectively, now incorporated as part of [802.1Q]. For all intents and purposes, claiming compliance to [802.1Q], [802.1ad], or [802.1ah] in the scope of this specification will be treated as claiming compliance to IEEE Std. 802.1Q-2011. Unless otherwise stated, claiming compliance to 802.1Q-2005 requires a specific date reference.

[802]	IEEE Std. 802-2001, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture, 2001.
[802.1]	Refers to entire suite of IEEE 802.1 standards unless otherwise specified.
[802.1AB]	IEEE Std. 802.1AB-2009, IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks – Amendment 6: Provider Backbone Bridges, 2009.
[802.1AE]	IEEE Std. 802.1AE-2006, IEEE Standard for Local and Metropolitan Area Networks: – Media Access Control (MAC) Security, 2006.
[802.1ah]	IEEE Std. 802.1ah-2008, IEEE Standard for Local and Metropolitan Area Networks – Station and Media Access Control Connectivity Discovery, January 2008. Former amendment to 802.1Q, now part of 802.1Q-2011.
[802.1d]	IEEE Std. 802.1d™-2004, IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Bridges
[802.1Q]	IEEE Std. 802. 1Q-2011, IEEE Standard for Local and Metropolitan Area Networks – Media Access Control (MAC) Bridges and Virtual Bridge Local Area Networks, August 2011.
[802.3]	IEEE 802.3-2008, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and Physical Layer specifications, January 2008.
[802.3ah]	IEEE 802.3ah™-2004: Amendment to IEEE 802.3™-2005: Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks, an amendment to [802.3].
[802.3av]	IEEE 802.3AV-2009, IEEE Standard for Information technology-Telecommunications and information systems-Local and metropolitan area networks-Specific requirements, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 1: Physical Layer Specifications and Management Parameters for 10Gb/s Passive Optical Networks.
[CANN-DHCP-Reg]	CableLabs DHCP Options Registry, CL-SP-CANN-DHCP-Reg, Cable Television Laboratories, Inc.
[CMCIv3.0]	Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, CM-SP-CMCIv3.0, Cable Television Laboratories, Inc.
[DPoE-IPNEv1.0]	DOCSIS Provisioning of EPON, IP Network Element Requirements, DPoE-SP-IPNEv1.0, Cable Television Laboratories, Inc.

[DPoE-MEFv1.0] DOCSIS Provisioning of EPON, Metro Ethernet Forum Specification, DPoE-SP-MEFv1.0, Cable Television Laboratories, Inc.

[DPoE-MULPIv1.0] DOCSIS Provisioning of EPON, MAC and Upper Layer Protocols Requirements, DPoE-SP-MULPIv1.0, Cable Television Laboratories, Inc.

[eDOCSIS] Data-Over-Cable Service Interface Specifications, eDOCSIS Specification, CM-SP-eDOCSIS, Cable Television Laboratories, Inc.

[G.805] ITU-T Recommendation G.805 (03/00), Generic functional architecture of transport networks.

2.2 Informative References

This specification uses the following informative references.

[802.1ad] IEEE Std. 802.1ad-2005™-2006, IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks Amendment 4: Provider Bridges, May 2006. Former amendment to 802.1Q, now part of 802.1Q-2011

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

[802.1ax] IEEE Std. 802.1ax-2008, IEEE Standard for Local and Metropolitan Area Networks – Link Aggregation, January 2008.

[802.3ac] IEEE Std. 802.3ac™-1995, IEEE Standard for Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications - Frame Extensions for Virtual Bridged Local Area Network (VLAN) Tagging on 802.3 Networks, January 1995. Now part of [802.3].

[802.3ag] IEEE Std. 802.3ag™-2007, IEEE Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks-Amendment 5: Connectivity Fault Management, January 2007.

[802.3as] IEEE Std. 802.3as™-2006, Amendment 3 to IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 3, November 2006.

[DOCSIS] Refers to DOCSIS 3.0 Specification unless otherwise specified.

[DPoE-ARCHv1.0] DOCSIS Provisioning of EPON, DPoE Architecture Specification, DPoE-SP-ARCHv1.0, Cable Television Laboratories, Inc.

[DPoE-OAMv1.0] DOCSIS Provisioning of EPON, OAM Extensions Specification, DPoE-SP-OAMv1.0, Cable Television Laboratories, Inc.

[DPoE-OSSIv1.0] DOCSIS Provisioning of EPON, Operations and Support System Interface Specification, DPoE-SP-OSSIv1.0, Cable Television Laboratories, Inc.

[DPoE-PHYv1.0] DOCSIS Provisioning of EPON, Physical Layer Specification, DPoE-SP-PHYv1.0, Cable Television Laboratories, Inc.

[DPoE-SECv1.0] DOCSIS Provisioning of EPON, Security and Certificate Specification, DPoE-SP-SECv1.0, Cable Television Laboratories, Inc.

[eRouter] Data-Over-Cable Service Interface Specifications, eRouter Specification, CM-SP-eRouter, Cable Television Laboratories, Inc.

[I2C]	UM10204, I²C-bus specification and user manual, Rev. 03, 19 June 2007, http://www.nxp.com/acrobat_download/usermanuals/UM10204_3.pdf.
[L2VPN]	Data-Over-Cable Service Interface Specifications, Layer 2 Virtual Private Networks, CM-SP-L2VPN, Cable Television Laboratories, Inc.
[MEF 6]	Metro Ethernet Forum, MEF 6.1 Ethernet Services Definitions, Phase 2, April 2008.
[MEF 9]	Metro Ethernet Forum, Abstract Test Suite for Ethernet Services at the UNI, October 2004.
[MEF 14]	Metro Ethernet Forum, Abstract Test Suite for Traffic Management Phase 1, November 2005.
[MEF 21]	Metro Ethernet Forum, Service OAM and Requirements Framework, Phase 1, April 2007.
[MEF 26]	Metro Ethernet Forum, External Network to Network Interface (ENNI) – Phase 1, January 2010.
[MULPIv3.0]	Data-Over-Cable Service Interface Specifications, MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.0, Cable Television Laboratories, Inc.
[OSSIv3.0]	Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification, CM-SP-OSSIv3.0, Cable Television Laboratories, Inc.
[PHYv3.0]	Data-Over-Cable Service Interface Specifications, Physical Layer Specification, CM-SP-PHYv3.0, Cable Television Laboratories, Inc.
[RFC 2011]	IETF RFC 2011, SNMPv2 Management Information Base for the Internet Protocol using SMIv2, K. McCloghrie, November 1996.
[RFC2132]	IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions, S. Alexander, March 1997.
[RFC 2863]	IETF RFC 2863, The Interfaces Group MIB, June 2000.
[RFC 3418]	IETF RFC 3418/STD0062, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), June 2000.
[RFC3986]	IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, T. Berners-Lee, January 2005.
[RFC 4188]	IETF RFC 4188, Definitions of Managed Objects for Bridges, September 2005.
[RFC 4293]	IETF RFC 4293, Management Information Base for the Internet Protocol (IP), April 2006.
[SCTE 174]	SCTE 174 2010, Radio Frequency over Glass Fiber-to-the-Home Specification.
[SECv3.0]	Data-Over-Cable Service Interface Specifications, Security Specification, CM-SP-SECv3.0, Cable Television Laboratories, Inc.
[SFF-8077i]	SFF-8077i 10 Gigabit Small Form Factor Pluggable Module, Revision 4.0, released April 13, 2004.
[SFF-8472]	SFF-8472 Specification for Diagnostic Monitoring Interface for Optical Transceivers, Revision 10.4, released January 2009.
[SFP MSA]	INF 8074i Rev 1.0, Small Form-factor Pluggable Multi-Source Agreement, released 12 May 2001.

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
- 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
- International Telecommunication Union (ITU), Place des Nations, CH-1211, Geneva 20, Switzerland; Phone +41-22-730-51-11; Fax +41-22-733-7256. Internet: http://www.itu.int
- 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: +1-800-542-5040, Fax: +1-610-363-5898, Internet: http://www.scte.org/
- Small Form Factor Committee (SFF), http://www.sffcommittee.com

3 TERMS AND DEFINITIONS

3.1 DPoE Elements

DPoE Network	This term means the entire network described in Figure 2 from the D or MN interface to the LCI, S, MI, or MU interface (see Figure 2 for interface and reference points), depending on the service being described. The DPoE Network includes the part of a DEMARC that supports DEMARC Auto Configuration.
DPoE System	This term means all the collected elements that provide the DPoE function within the operator's network facilities. This includes the EPON OLT function, DOCSIS service functions required for the D interface, Metro Ethernet service functions required for the MN interface, and IP NE element management, routing and forwarding functions specified in [DPoE-IPNEv1.0]. The DPoE System is depicted in Figure 4.
DPoE ONU (D-ONU)	This term means a DPoE-capable ONU that complies with all the DPoE specifications. There are two logical types of D-ONUs. These are the DPoE Standalone ONU and the DPoE Bridge ONU.
DPoE Standalone ONU (S-ONU)	This term means a D-ONU that provides all the functions of a B-ONU and also provides at least one CMCI port. An S-ONU can optionally have one or more eSAFEs.
DPoE Bridge ONU (B-ONU)	This term means a D-ONU that is capable of [802.1] forwarding but cannot do all the encapsulation functions required to be a DPoE Standalone ONU. The B-ONU is a logical definition used by the specification for requirements that apply to all types of B-ONUs. The two types of B-ONUs are the BP-ONU and the BB-ONU.
DPoE Bridge Pluggable ONU (BP-ONU)	This term means a D-ONU that is a B-ONU that is pluggable. Pluggable BP-ONUs include devices such as an SFP-ONU (1G-EPON), SFP+ONU (10G-EPON), or XFP-ONU (10G-EPON).
DPoE Bridge Baseband ONU (BB-ONU)	This term means a D-ONU that is a B-ONU that has a baseband IEEE Ethernet interface. BB-ONUs include those with one or more [802.3] baseband PMDs. (See [DPoE-ARCHv1.0], section 7.2.6.2 for examples.)
DEMARC	Short form of "Demarcation Device." This term means the device, owned and operated by the operator that provides the demarcation (sometimes called the UNI interface) to the customer. Some architectures describe this device as the CPE (as in DOCSIS) or the NID (as in the MEF model).

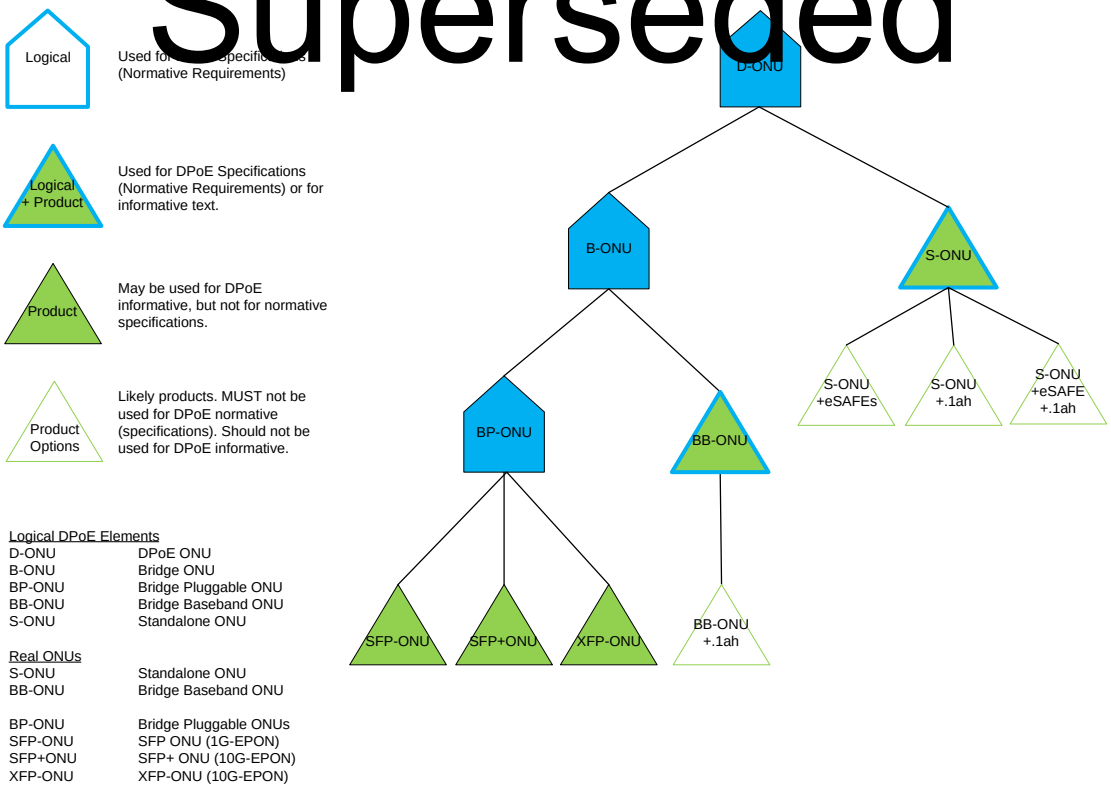

Figure 3 - D-ONU Types

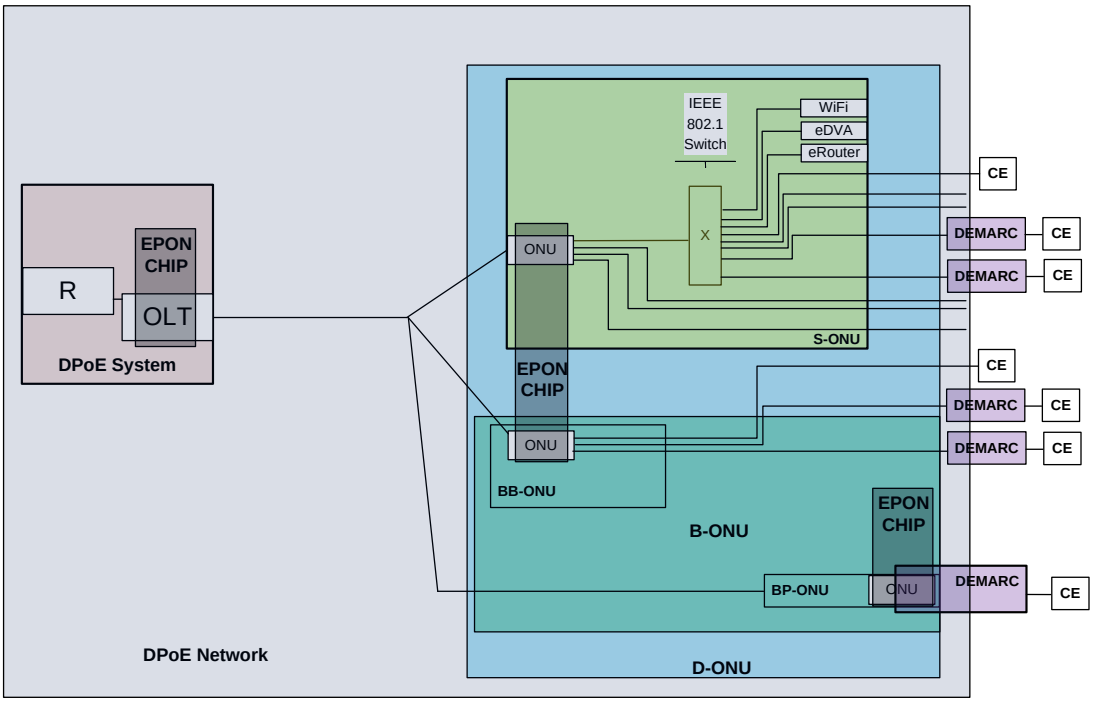

Figure 4 - DPoE Elements

3.2 Other Terms

1G-EPON	EPON as defined in [802.3ah]
10G-EPON	EPON as defined in [802.3ah] and amended in [802.3av]
Cable Modem CPE Interface	CMCI as defined in [MULPIv3.0]
Customer Equipment	Customer Equipment as defined in [DPoE-MEFv1.0]
Customer Premise Equipment (CPE)	Customer Premise Equipment as defined in [DOCSIS]
Ethernet Passive Optical Network (EPON)	Refers to both 1G-EPON and 10G-EPON collectively
EPON Operations and Maintenance Messaging (OAM)	EPON OAM messaging as defined in [802.3ah] and [DPoE-OAMv1.0]; Ethernet OAM is not the same as EPON OAM; Ethernet OAM is [802.1ag].
Network Interface Device (NID)	A DEMARC in DPoE specifications

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

BOOTP	Bootstrap protocol
CMCI	Cable Modem CPE Interface
CE	Customer Equipment
CPE	Customer Premise Equipment
DA	Destination Address
DAC	DEMARC Automatic Configuration
DDMI	Digital Diagnostic Monitoring Interface
DDMM	Digital Diagnostic Memory Map
DHCP	Dynamic Host Configuration Protocol
DPoE	DOCSIS Provisioning of EPON
DR	Default Router
EPL	(E-LINE) Ethernet Private Line
EPON	Ethernet Passive Optical Network
EMS	Element Management System
EVC	Ethernet Virtual Connection
E-VPL	Ethernet Virtual Private Line
IP(HSD)	High Speed Data (Broadband Internet Access using DOCSIS)
I-NNI	Internal Network to Network Interface
IP	Internet Protocol
I-SID	[802.1ah] I-Component Service Identifier
LCI	Logical CPE Interface
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LLID	Logical Link Identifier
MAC	Media Access Control (sublayer)
MEF	Metro Ethernet Forum
MEN	Metro Ethernet Network
MI	MEF I-NNI Interface
MLS	Multi-Layer Switching
MN	MEF I-NNI Interface to operators' MEN
MU	MEF UNI Interface
NID	Network Interface Device
NNI	Network to Network Interface
NMS	Network Management System
OAM	EPON Operations Administration and Maintenance
ODN	Optical Distribution Network

OLT	Optical Line Termination
ONU	Optical Network Unit
OSS	Operations and Support Systems
PB	Provider Bridging [802.1ad]
P2P	Point-to-Point
P2PE	Point-to-Point Emulation
PHY	Physical Layer
PMD	Physical Media Dependent (Sublayer)
PON	Passive Optical Network
QoS	Quality of Service
R	IP Router
SA	Source Address
SFP	Small Form-factor Pluggable
SFF	Small Form-Factor Committee
SFP-ONU	Small Form-factor Pluggable ONU
SFP+	Small Form-factor Pluggable Plus (+)
SFP+ ONU	Small Form-factor Pluggable Plus (+) ONU
SFTP	Secure File Transfer Protocol
SSH	Secure Shell
UNI	User Network Interface
URI	Uniform Resource Identifier
vCM	Virtual Cable Modem
WDM	Wavelength Division Multiplexing
X	IEEE Ethernet Switch (Generic)
XFP	X Form-factor Pluggable
XFP-ONU	X Form-factor Pluggable ONU

5 DEMARC IN THE DPOE NETWORK

5.1 Background

The process of manually creating, distributing, and updating configuration files is time-consuming and prone to operator error and other challenges. One of the challenges of provisioning a device at the customer premises is the fact that there is no industry standard solution for provisioning Ethernet devices.

There are two widely used industry standards for IP-based automatic device configuration. These are the bootstrap protocol (BOOTP) and the Dynamic Host Configuration Protocol (DHCP). Both solutions assume that the device in question is attached to an IP network. While this is a valid assumption for IP network-based services (like Internet access or IP-VPNs) it is not a valid assumption for Metro Ethernet services, where automated allocation of VLAN IDs is needed and currently not provided by any existing Ethernet protocol. When Metro Ethernet services are offered, typically with an Ethernet access network technology, multiple Ethernet services can be multiplexed over the access network. For example, if a DEMARC is used in a Multiple Tennant Unit environment, it is desired to separate the provisioning of the management path to the DEMARC and provisioning of the DEMARC from the provisioning of services for individual customers. In particular, the requirement is to de-couple the provisioning of the DEMARC in-band management path from the CM provisioning process (which is typically associated with individual customers). The challenge is that there is no standard means to identify which Ethernet service (in the case of MEF – which Ethernet Virtual Connection (EVC)) should be used for management, versus those used for UNI forwarding.[1]Even if an operator followed a recommendation of MEF, suggesting to use VID 4090 for this purpose, such recommendations are based on the assumption that the Ethernet access link is dedicated. There are no provisions for how to handle the in-band management traffic when that traffic is present on a platform like the DPoE System (or any OLT or switch) where there are multiple such VIDs. There are additional security, operational, and scaling concerns when using a single C-VLAN ID for in-band management across multiple DEMARC devices.

In an access network, the DEMARC is located in the customer premises and typically is either the access network termination device or is attached to an access network termination device. Either the DEMARC or the access network termination device has connectivity to the operator's network across an access network interface. In a DPoE Network, the access network interface corresponds to the TU interface.

For Metro Ethernet services, the TU interface carries one or more logical Ethernet services, organized into EVCs as described by MEF. By definition, the EVC carries Ethernet frames from one UNI to another. The problem for operators is how to have an IP connection for managing the DEMARC that is outside of any of those EVCs. More specifically, the problem is how to automate a standard method of providing an IP connection in-band on the TU interface.

The solution cannot be as simple as a "default VLAN" because a single VLAN cannot be used on a shared network (a PON) across multiple devices, and still be unique for each premises or for each DEMARC. Even where it is possible to operate a single VLAN across multiple devices, operating a single VLAN (which is a single broadcast domain) across multiple DEMARC devices and multiple premises presents multiple operational, scaling and security concerns. The operators require a dedicated Ethernet control path (established using any specified combination of [802.1Q][2] tagging for Ethernet frames) for each DEMARC in order to segregate management traffic from regular subscriber traffic in order to meet security and other operational needs.

In addition, a method for identifying a configuration file for a DEMARC is not standardized.

This specification provides requirements to solve the above problems by specifying a method for the automation of in-band DEMARC management over the DPoE Network, providing the name for the DEMARC configuration file, and the means for file transfer from the OSS to the DEMARC over the DPoE Network, therefore creating a DEMARC Automatic Configuration (DAC) mechanism.

[1] The Metro Ethernet Forum (MEF) Ethernet Access Services Definition D0.96 recommends the use of VLAN ID = 4090 for in-band management of service-provider devices. An operator can use VLAN ID 4090 for in-band management by provisioning the DAC Serving Group for VID=4090.

[2] Please see the note on the [802.1Q] standard compliance in subsection 2.1.

5.2 DEMARC Dependency on D-ONU

Configuration of the DEMARC also needs to meet other operator requirements and requirements based on the operation of other DPoE Network elements. For example, DAC cannot begin until after the D-ONU is configured and operational. If the D-ONU is not registered and operating, there is no means to establish an IP forwarding path from the OSS to the DEMARC.

It remains possible to provision and operate a DEMARC by implementing an out-of-band management path to the DEMARC; for example, by using a CM, telephone line and modem, or other means to connect to a serial port, Lights Out Management, or an Ethernet management port used with alternative access architectures.

5.3 DEMARC Interface Independence

Another goal of the specification is for the automatic configuration to work across any pluggable or baseband Ethernet interface. The method also needs to work with existing deployed B-ONUs, including both BP-ONUs and BB-ONUs.

6 DEMARC BASIC REQUIREMENTS

The DEMARC is a DPoE Element used to provide Metro Ethernet UNI services to business or commercial service customers. The requirements contained herein are the minimum requirements for a DEMARC to provide Metro Ethernet services (as defined by MEF) with automatic DEMARC discovery and configuration to both operate the services for the customer and configure the DEMARC for IP-based management by the operator.

Figure 1 shows a simplified DPoE Network with DPoE System, a D-ONU providing MU and a DEMARC. The D-ONU provides an MI interface to a DEMARC. The DEMARC has the MI interface to the D-ONU and an MU interface for Metro Ethernet service connected to the CE.

6.1 DPoE Metro Ethernet Service

DEMARCs MUST support the MEF UNI (MU) interface requirements specified for a D-ONU in [DPoE-MEFv1.0].

6.2 Metro Ethernet Service Requirements

The DEMARC MUST support the IEEE specifications as defined for a D-ONU in [DPoE-MEFv1.0].

6.3 Metro Ethernet Forum Standards

The DEMARC MUST support the MEF specifications as defined for a D-ONU in [DPoE-MEFv1.0].

6.4 IP Network Element Requirements

The DEMARC SHOULD support the same IP management service requirements defined for a DPoE System in [DPoE-IPNEv1.0]. Examples of these types of services include Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Trivial File Transfer Protocol (TFTP), Secure HTTP (HTTPS), SNMPv2, SNMPv3, SYSLOG, etc.

6.5 DEMARC Auto-Configuration Requirements

The DEMARC MUST support DEMARC Auto-Configuration as defined in this specification.

7 IP MANAGEMENT FOR A DEMARC

In this version of the DPoE specifications, the IP over-the-top model for establishing a control path with the DEMARC remains unspecified. This specification provides a method for provisioning an Ethernet control path to the DEMARC, relying on [802.1Q] tagging. With DPoE version 1.0 specifications, an operator can provision an Ethernet Private Line (EPL) as illustrated in Figure 5 (orange line) and use that EVC to run Ethernet or IP-based management of the DEMARC over the top of the DPoE Network. In such a case, the operator must provision the EVC in the D-ONU (vCM) configuration file.

Additionally, this version of the DPoE specification introduces an automated method of identifying a DEMARC, creating an Ethernet path from the DPoE System to the DEMARC, assigning an IP address to the DEMARC, initiating a file transfer for a configuration file, and making the DEMARC available as an IP device connected to the DPoE System IP router (R), as illustrated in Figure 5 (purple line). This automated method is hereafter referred to as DEMARC Auto Configuration (DAC).

In this version of the DPoE specification, the DPoE Network may be provisioned with a dedicated Ethernet path from the DPoE System through the D-ONU to the DEMARC.

The DPoE Network MUST use PB to establish a data path between the DEMARC, through D-ONU to the DPoE System. When PB is used, one or more S-VLANs are allocated for DAC and a dedicated C-VLAN (from that allocated S-VLAN) is used for each DEMARC. The S-VLANs are assigned to a DAC Serving Group. Within the serving group, the DPoE System autonomously allocates C-VLANs.

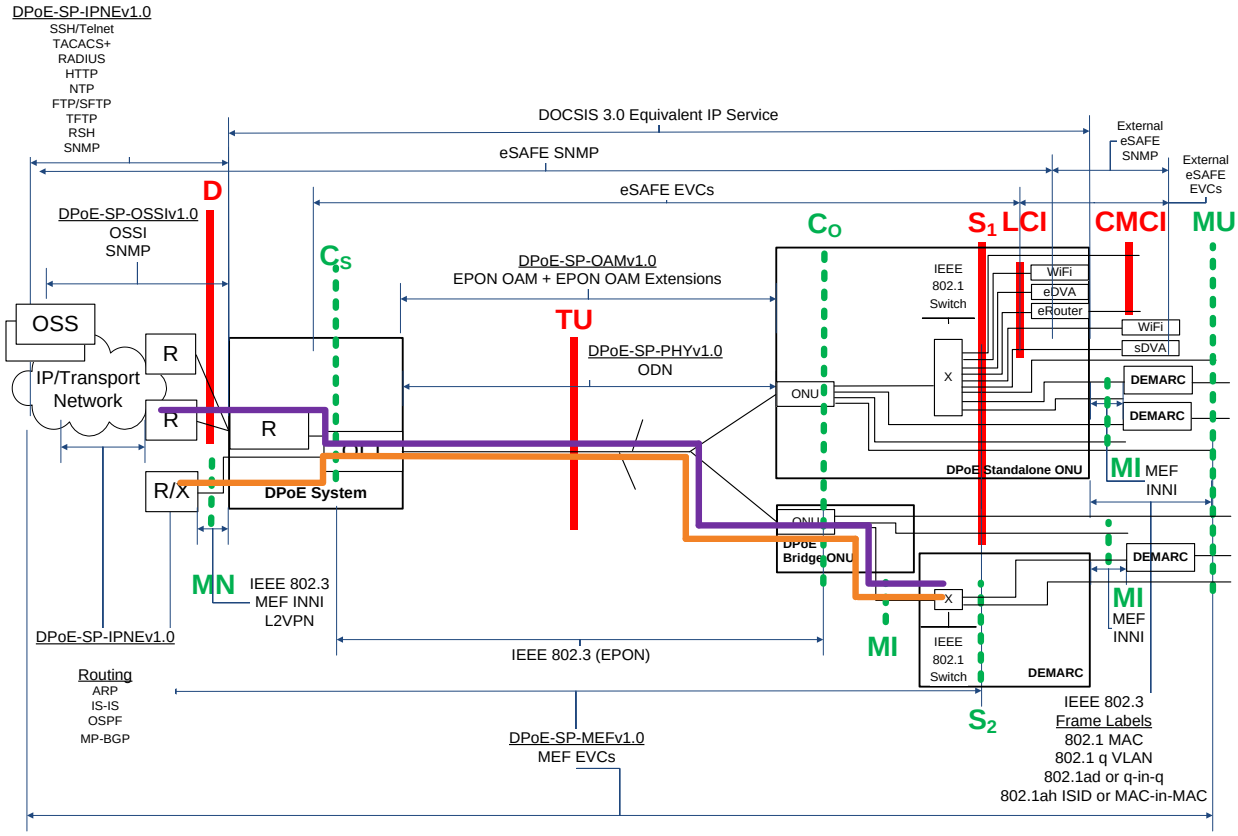

Figure 5 - DPoE Network Showing the Metro Ethernet Service Forwarding Path from MN to MU

8 DEMARC AUTO-CONFIGURATION (DAC)

8.1 Introduction to DAC

The DAC process provides means for the automatic discovery, configuration of an in-band IP management service, and the discovery and transfer of a configuration file specific to the particular DEMARC that is discovered and connected.

As with DOCSIS, this specification does not describe the means to generate a configuration file for the D-ONU and the DEMARC. A DEMARC configuration file is required for a file transfer to occur. The configuration file may be generated at any time prior to the file transfer.

8.1.1 DAC Architecture and Overview

By definition, a DEMARC is an Ethernet device that connects to the MI interface of a D-ONU and provides one or more MU interfaces on a DPoE Network (as depicted in Figure 5 above). Figure 6 shows an example of a BB-ONU or S-ONU connected to a DEMARC.

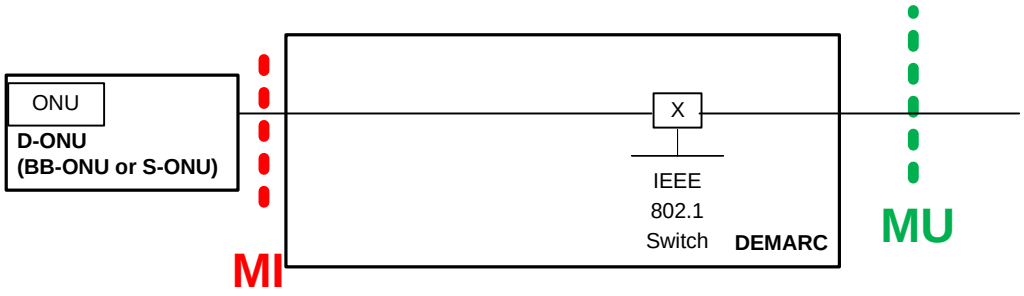

Figure 6 - BB-ONU or S-ONU

In the scope of this specification, the operations of the S-ONU and a BB-ONU are considered to be identical. The operation of a BP-ONU requires additional specifications because of the BP-ONU's dependency on the DEMARC for electrical power, certain functions of the combined operations, and enabling of the pluggable (BP-ONU) interface. Figure 7 shows the relationship between the DEMARC and the BP-ONU, together with the location of the MI interface within the DEMARC.

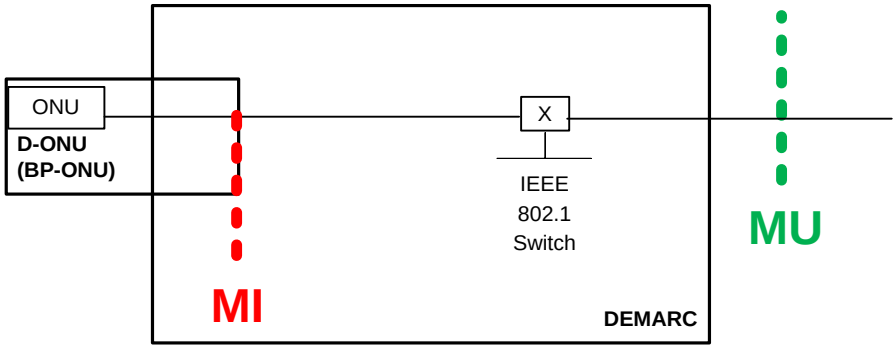

Figure 7 - BP-ONU

For example, the DEMARC can enable or disable the port, configure transceiver parameters, and read current transceiver status information. Note that the DPoE-SP-OSSIv1.0 specification specifically prohibits the configuration of the D-ONU from the UNI interface for CMCI or MU.

The goal for DAC is to provide automatic discovery of the presence of and provisioning for a DEMARC. Following is a summary of the steps required to meet this goal. As shown in Figure 5 above, DAC requires communication between each DPoE Element in sequence to build an IP over Ethernet forwarding path to the DPoE System and ultimately to the OSS, for initial configuration. The DPoE System, D-ONU, and DEMARC need to perform the following actions:

1. Start-up the DEMARC and D-ONU.
2. D-ONU registers and is provisioned according to [DPoE-MULPIv1.0].
3. D-ONU communicates configuration information to the DEMARC using [802.1AB] Link Layer Discovery Protocol (LLDP) protocol with DPoE-specific TLVs. This facilitates the setup of an Ethernet path between the DPoE System and the DEMARC to be used as a management path. The Ethernet path for DEMARC management terminates at the IP router on the DPoE System. From there, the DPoE System D interface provides IP forwarding from the DPoE System IP routing instance to the OSS.
4. The DEMARC transmits DHCP Discover message over the management path.
5. The DHCP Server responds to the DHCP message by sending a DHCP Offer or ACK message. These messages are modified by the DPoE System to insert the address to the required service configuration file. The DHCP messages are then forwarded to the DEMARC using the management path.
6. The DEMARC requests the service configuration file using a secure file transfer protocol and path that was provided in the DHCP ACK messages.
7. The DEMARC receives the service configuration file via a secure file transfer protocol, parses the received file, and configures its ports, together with the associated services as requested.

More detail on the DAC process is provided in the next section.

8.1.2 DAC Operation Detailed Description

The method of operation varies across different types of D-ONUs. There are common specifications that apply to all D-ONUs. Additionally, there are specifications particular to specific types of D-ONUs, such as those for a BB-ONU or those for a BP-ONU. DAC specifications are applicable to D-ONU ports configured to operate as an MI interface only.

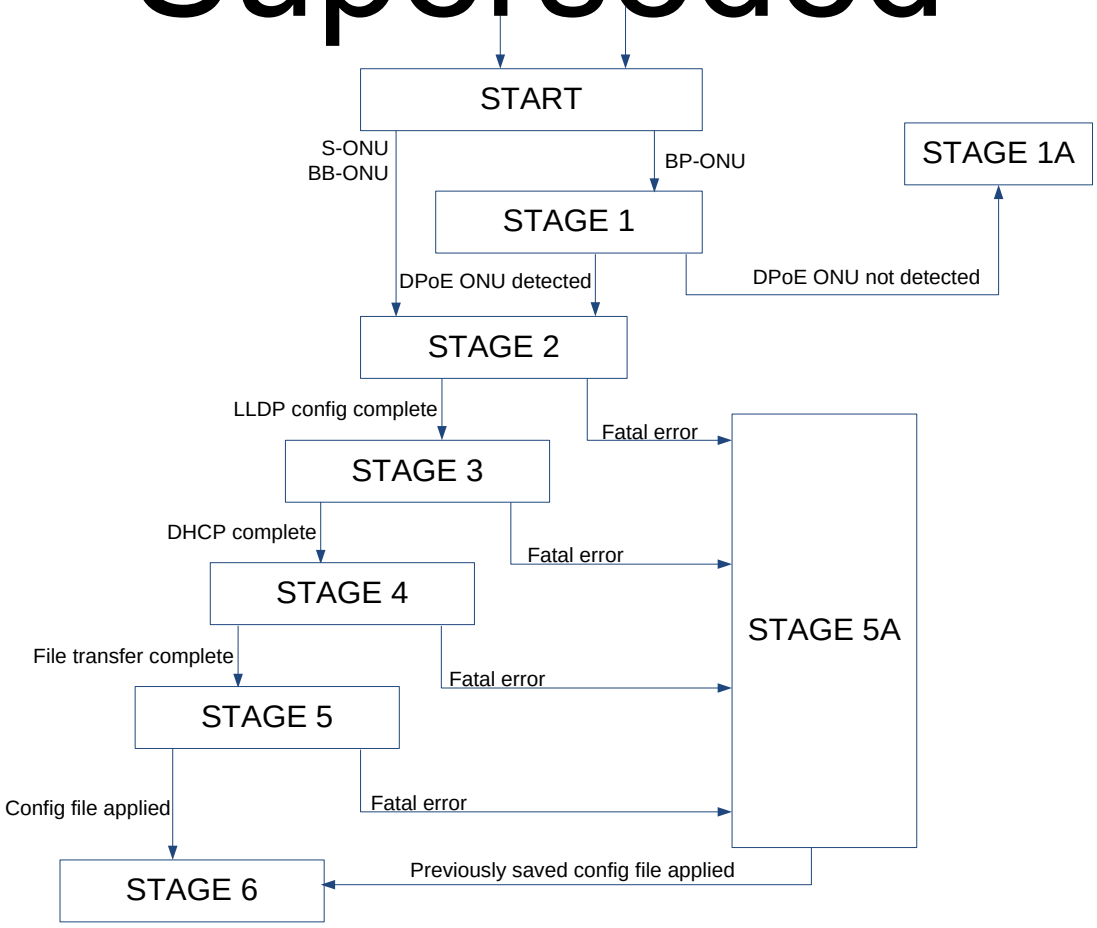

Figure 8 - Flow Chart for DAC

Figure 8 shows the flow diagram of the DAC process. Individual stages of the process are described in more detail in the following sections.

8.1.2.1 STAGE 1

Application of power to the DEMARC and D-ONU initiates Stage 1. An S-ONU or BB-ONU might be powered on separately or be already powered at this stage, whereas a BP-ONU receives power from the DEMARC. For simplicity of description, it is assumed that the DEMARC and the S-ONU are powered on simultaneously. At this time, both devices initialize and perform basic internal configurations, check-ups, etc., required for their proper operation.

Stage 1 is dedicated to confirming the type of transceiver plugged into the DEMARC. After completing Stage 1, the DEMARC should be able to distinguish the BP-ONU from a standard P2P transceiver in the appropriate form factor.

If the DEMARC is connected to a BP-ONU, the DEMARC performs the discovery of the BP-ONU plugged into the receptacle using the communication interface typically used by the pluggable transceivers. As an example, BP-ONUs housed in SFP-type transceivers use the [I2C] bus to exchange information between the DEMARC and the optical transceiver. Additional information on the process of identification of the SFP, SFP+, and XFP type BP-ONUs are included in 8.1.2.1.1 and 8.1.2.1.2.

During the start-up phase, the DEMARC verifies the presence, current administrative status, and a series of other parameters as indicated in the memory map (including such parameters as temperature, bias current, manufacturer, version, model, power range, device status, etc.) stored on a compliant transceiver. [SFF-8472] defines the memory

map for the SFP and SFP+ compliant transceivers. [SFF-8077i] defines the memory map for the XFP-compliant transceivers.

To distinguish the transceiver equipped with an EPON chipset (i.e., BP-ONU) from other typical transceivers used for Point-to-Point (P2P) CWDM/DWDM communication, the DPoE-specific information can be read from a predefined location in the transceiver memory map, as identified in more detail in 8.1.2.1.1 and 8.1.2.1.2.

If the DEMARC is connected to an S-ONU, it is unnecessary to attempt communication with a BP-ONU; the DEMARC can proceed directly to Stage 2.

8.1.2.1.1 SFP-ONU and SFP+ONU

The DEMARC is capable of identifying a BP-ONU across the [I2C] bus, operating between the BP-ONU host and the BP-ONU as described in [SFF-8472] for SFP and SFP+ type transceivers.

The Digital Diagnostic Monitoring Interface (DDMI) operates over [I2C] using the Digital Diagnostic Memory Map (DDMM) as an address based memory map for individual data fields, representing specific parameters for the given transceiver type. Figure 3.1 in [SFF-8472] presents the structure of the individual DDMM fields for SFP and SFP+ transceivers.

In [SFF-8472], the DDMM memory space is available at the address of 0xA0 Bytes 3-10 and byte 36 at the address of 0xA0 contains the transceiver compliance codes. These bytes are bit-selective. At least one bit has to be set to define protocol and bit-rate of the physical device. Additional details can be found in Table 3.1 and Table 3.1a in [SFF-8472].

To identify new transceiver types for BP-ONUs used in the DPoE Network, new code points (as defined in respective SFF specification) are needed. The new transceiver identifiers, to be inserted into Table 3.2 (byte 0 at the address of 0xA0) in [SFF-8472], are shown in Table 3. The new transceiver types, to be inserted into Table 3.5 (byte 36 at the address of 0xA0) in [SFF-8472], are shown in Table 4. Individual transceiver types shown in this table are identified in a bit-map fashion, where each bit position in byte 36 is used to represent one of the possible transceiver types.

Table 3 - New Transceiver Types for [SFF-8472] BP-ONUs

A0h data address	Value	Description of physical device
0	0x0D	EPON SFP ONU
	0x0E	10G-EPON SFP+ ONU
	0x0F	10G-EPON XFP ONU

Table 4 - New Transceiver Types for BP-ONUs

A0h data address	Bit	Description of transceiver
36	2-7	Unallocated
	1	10GBASE-PRX
	0	10GBASE-PR

A DEMARC can easily discover and identify a BP-ONU using the transceiver identifiers, types and serial ID information defined by [SFF-8472]. Table 5 illustrates examples of code point allocation for different BP-ONU types.

Table 5 - Examples of Code Point Allocation for Different SFP BP-ONU types

PMD Type	Form Factor	Identifier A0[0]	Transceiver code	Encoding A0[11]	Length A0[14] (SMF, km)
PX10	SFP	0x0D	A0[6] = 0x80	0x01	0x0A
PX20	SFP				0x14
PX20+	SFP				0x1E
PRX10	SFP+	0x0E	A0[36] = 0x02	0x06	0x0A
PRX20	SFP+				0x14
PRX30	SFP+				0x1E
PR10	SFP+	0x0E	A0[36] = 0x01	0x06	0x0A
PR20	SFP+				0x14
PR30	SFP+				0x1E

8.1.2.1.2 XFP-ONU

[SFF-8077i] uses the same DDMI interface as defined in [SFF-8472]. Figure 28 in [SFF-8077i] presents the structure of the individual DDMM fields for XFP transceivers.

Although the memory map is structured differently, [SFF-8077i] shares the same identifier values as defined in [SFF-8472]. It also has bit-selective bytes (Table 0x01, byte 131-138) for transceiver compliance codes. Table 6 shows new transceiver compliance codes for BP-ONUs that need to be added into [SFF-8077i]. Individual transceiver types shown in this table are identified in a bit-map fashion, where each bit position in byte 36 is used to represent one of the possible transceiver types.

Table 6 - New Transceiver Types for [SFF-8077i] BP-ONUs

Table 0x01 data address	Bit	Description of transceiver
133	2-7	Unallocated
	1	10GBASE-PRX
	0	10GBASE-PR

Similarly, DEMARC can easily discover and identify XFP-ONUs, if present. Table 7 illustrates examples of code point allocation for different BP-ONU types.

Table 7 - Examples of Code Point Allocation for Different XFP BP-ONU types

PMD Type	Form Factor	Identifier A0[0] and A0[128] ID data table 01h	Transceiver code (ID data table 01h)	Encoding A0[139] (ID data table 01h)	Length A0[142] (SMF, km)
PRX10	XFP	0x0F	A0[133] = 0x02	0x80	0x0A
PRX20	XFP				0x14
PRX30	XFP				0x1E
PR10	XFP	0x0F	A0[133] = 0x01	0x80	0x0A
PR20	XFP				0x14
PR30	XFP				0x1E

8.1.2.2 STAGE 1A

If the DEMARC fails to detect a BP-ONU in the receptacle or a standard (non DPoE ONU) transceiver is detected, the DEMARC MUST load the appropriate start-up file and continue its operation in a manner identical to operation in the absence of a D-ONU. This guarantees that the DEMARC can still operate with existing transceiver types.

8.1.2.3 STAGE 2

In this stage, the DEMARC needs to discover the Ethernet link configuration parameters for the connection between the DEMARC and the D-ONU. The link parameters include the required encapsulation format (as configured by an operator), D-ONU port mode (encapsulation or transport), as well as additional required information to make sure that the DEMARC can successfully transmit the DHCP Discover message to the back office system.

To achieve this, the DEMARC implements the [802.1AB] LLDP Receiver agent, capable of receiving the Link Layer Discovery Protocol Data Units (LLDPDUs) from the D-ONU, parsing the DPoE-specific TLV and performing its local configuration.

The DEMARC also implements the [802.1AB] LLDP Transmitter agent to support bidirectional LLDP transmission as required by the [802.1AB] standard.

The D-ONU implements the [802.1AB] LLDP Transmitter agent, capable of generating the LLDPDU with attached DPoE-specific TLV, containing information about the link configuration requirements for the given D-ONU. The structure of the DPoE-specific TLVs is discussed in more detail in Annex A of this specification.

The D-ONU implements the [802.1AB] LLDP Receiver agent to support bidirectional LLDP transmission as required by the [802.1AB] standard.

Once the D-ONU comes online and it is successfully configured by the network operator, the LLDP Transmitter agent starts sending LLDPDUs using the multicast destination address, as allowed by the [802.1AB] LLDP standard, on the port connected to the DEMARC. In case of S-ONUs equipped with multiple ports, the S-ONU MUST operate an independent LLDP agent on each port to allow for transmission of the LLDPDU across the link to the connected DEMARC. The process is continuous, and its frequency is implementation dependent.

Once the DEMARC receives an LLDPDU with the DPoE-specific TLV, it parses it and identifies the requirements for the port configuration to allow for the transmission of the DHCP Discover message to the OSS. The information retrieved from the LLDPDU includes: (a) whether the DPoE ONU is configured to operate in the encapsulation or transport mode, (b) what [802.1Q] tagging needs to be applied to any DHCP message on the DEMARC to allow for successful forwarding through the DPoE ONU, etc. The DEMARC uses this information to configure the port forwarding of frames through the D-ONU onto the DPoE Network. All DHCP messages generated by the software agent operating on the DEMARC are processed and encapsulated in a manner consistent with the D-ONU default configuration requirements as delivered using the DPoE-specific TLV in the LLDPDU.

In case of an S-ONU, each MI-type port must be configured with dedicated Ethernet configuration path parameters. This allows each DEMARC connected to such S-ONU ports to be uniquely recognized by the OSS and configured independently.

The D-ONU SHOULD NOT start any LLDP sessions until it powers up, completes any initialization and boot sequences, giving it enough time to initialize itself before starting transmission of the LLDPDUs on the port connected to the DEMARC

When the LLDP configuration process successfully completes, an Ethernet path between the DEMARC and DPoE System has been set up, representing the completion of Stage 2. If the DEMARC is unable to obtain configuration parameters via LLDP, the DEMARC MUST apply the retry mechanism as specified in Section 9.1.1.

In case of any fatal error condition detected during the operation of the DAC process, the DEMARC MUST transition to STAGE 5A, as shown in Figure 8. It is up to the DEMARC implementer to determine what constitutes a fatal error during the operation of the device.

8.1.2.4 STAGE 3

In this stage, the DEMARC executes the DHCP process. The DHCP Discover and DHCP Request messages sourced from the DEMARC are suggested to carry a number of populated option fields, including the unique identification of the DEMARC, comprising its MAC address or any other unique identifier allowing the back office system to distinguish this particular DEMARC from any other such device on the network.

Additionally, the DHCP Discover and Request messages may also include a list of DEMARC capabilities. The contents of the DHCP Discover and DHCP Request messages (options and sub-options) should be unique for the given DEMARC and provide enough information to the back office system to properly establish capabilities of this device and generate the service configuration file.

The DHCP Discover message is broadcast on the DEMARC port connected to the D-ONU using the [802.1ad] configuration parameters delivered via LLDP in Stage 2.

When the DEMARC completed the DHCP process, it has obtained an IP address and configuration file information from the DHCP messages. When this information is obtained, Stage 3 is complete. If the IP address and configuration file information are not acquired by the DEMARC during the DHCP process, the DEMARC MUST apply the retry mechanism as specified in Section 9.1.1.

In case of any fatal error condition detected during the operation of the DAC process, the DEMARC MUST transition to STAGE 5A, as shown in Figure 8. It is up to the DEMARC implementer to determine what constitutes a fatal error during the operation of the device.

8.1.2.5 STAGE 4

In this stage, the DEMARC attempts to download a service configuration file from the OSS. The contents of the DEMARC configuration file, and the process for generating the configuration file, are outside the scope of DPoE specifications.

Such a service configuration file is then delivered to the DEMARC via the DPoE Network, as defined in the [DPoE-ARCHv1.0], with the appropriate [802.1Q] tagging. At that time, D-ONU forwards towards the DEMARC the individual frames comprising the configuration file using the default forwarding rules on the D-ONU for the given Ethernet path.

Successful download of the DEMARC configuration file represents the completion of Stage 4. If for any reason the configuration file fails to be downloaded, the DEMARC MUST apply the retry mechanism as specified in Section 9.1.1.

8.1.2.6 STAGE 5

In this stage, the DEMARC parses the configuration file, optionally verifies for any potential errors and processes it, performing its local configuration, opening necessary communication paths between the DEMARC and the D-ONU across the MI interfaces as needed.

The default configuration path between the DEMARC and the D-ONU established in Stages 2-3 remains open as long as the DEMARC and the D-ONU are powered on. This allows the OSS to update the configuration on the DEMARC as needed (e.g., establish new services for the customer, perform modifications, changes to QoS policies, etc.) without requiring physical access to the D-ONU or DEMARC.

The D-ONU maintains the LLDP on the DEMARC – DPoE ONU link operational as long as it is powered, using the LLDP refresh mechanism (see Stage 6 for more details).

Application of the configuration file represents completion of Stage 5 and the DEMARC transitions to Stage 6. If the configuration file is unable to be applied, the DEMARC MUST apply the retry mechanism as specified in Section 9.1.1.

In case of any fatal error condition detected during the operation of the DAC process, the DEMARC MUST transition to STAGE 5A, as shown in Figure 8. It is up to the DEMARC implementer to determine what constitutes a fatal error during the operation of the device.

8.1.2.7 STAGE 5A

Stage 5A represents a state in which the DEMARC recovers from a fatal stage error condition. In Stage 5A, the DEMARC MUST load a previously saved configuration file and continue operation.

8.1.2.8 STAGE 6

Stage 6 represents a normal operating mode. In this stage, either a newly downloaded configuration file is applied, or a previously saved configuration file is loaded. In either case, the DEMARC is in normal operating mode.

In this stage, the D-ONU SHOULD continually transmit the LLDP information on the port connected to the DEMARC at least once every two (2) seconds to provide an indication to the DEMARC that the D-ONU is still operational, and also to provide LLDP configuration information if the DEMARC reboots at any time.

9 DAC REQUIREMENTS

9.1 DEMARC Requirements for DAC

9.1.1 Retry mechanism

Unless otherwise noted, the DEMARC MUST support the following general retry process before declaring a "Fatal stage error" (see Figure 8) in the DAC process. The DEMARC MUST attempt to complete the processing for a stage at most five (5) times. On the fifth (6^{th}) stage error in a particular stage, a fatal stage error is declared.

The DEMARC MUST enter a message in an internal log each time the stage is attempted.

A stage error is declared if the DEMARC remains in the stage for three (3) seconds without completing the stage. During this time, there is no observed change in the state of the device, or any other activity. The three (3) second stage timeout requirement does not apply to normal and reasonable message exchanges to complete a particular process. For example, normal file transfer protocol timeouts are used to declare when a configuration file download attempt is in error.

During each stage of DAC, the DEMARC MUST implement a retry process to allow recovery from any error condition.

If the retry mechanism is initiated, the DEMARC MUST start a 3-second timer. At the end of the 3-second timer, the DEMARC MUST log a “Warning” message to a local log facility and attempt the previously failed action.

If after 5 attempts, the DEMARC is still unable to complete the failed action, the DEMARC MUST report a “Failure” to a local log facility.

Protocol and message exchange actions must follow the normal timeout and retry procedures defined by the respective protocol. In the case of file transfers (for example, TFTP, FTP, HTTP), the DEMARC MUST consider any failure returned by the protocol as an attempted transfer (for example timeouts, access denied, file not found) and continue the retry process as defined in this section. The DEMARC MUST NOT attempt the transfer more than five times.

9.1.2 General requirements

The DEMARC MUST implement [802.1AB] LLDP Transmitter and Receiver agents.

The DEMARC MUST transmit response LLDPDU with a source address of the DEMARC MAC address. In response LLPDUs, the DEMARC MUST set the destination MAC address equal to the source MAC address of the request LLPDUs.

The DEMARC MUST apply the [802.1Q] tagging information received from the LLDP configuration (Stage 2) to management frames, excluding LLDPDUs exchanged between the DEMARC and D-ONU.

The DEMARC MUST provide its chassis MAC address to the DHCP client as the MAC source address that is reachable across all Ethernet interfaces on the DEMARC that can be used as an MI interface. The DEMARC MAC address is expected to be a globally unique (assigned) MAC address as specified in [802]. In this specification, this MAC address is also referred to as the *chassis MAC address*.

9.1.3 File transfer requirements

The DEMARC MUST support TFTP file transfer mode for insecure file transfer mechanism. The DEMARC MUST support [SFTP] and [HTTPS] file transfer modes for secure file transfer mechanism.

The DEMARC MUST request the Secure File Transfer URI Option by inserting the CableLabs Vendor-Specific “Option Request” Option defined in [CANN-DHCP-Reg] into the DHCP Request message.

The DEMARC MUST initiate a file transfer of the DEMARC configuration file after the IP address and the configuration file name were obtained from the DHCP server via the Secure File Transfer URI Option carried in the DHCP Offer and Ack messages. The file name, file transfer protocol and the server address are derived from the Secure File Transfer URI Option, and this information is used to initiate the configuration file transfer. This information is to be used as follows.

If the Secure File Transfer URI Option is present in the DHCP Offer and ACK messages, the DEMARC MUST operate as follows:

- The DEMARC MUST use the secure file transfer mode indicated in the Secure File Transfer URI Option.
- If the secure file transfer mode selected by the Secure File Transfer URI Option is not supported by the DEMARC or fails for whatever reason, the DEMARC MUST go through the retry mechanism as defined in 9.1.1. If the secure file transfer mode fails to establish connectivity at the end of the retry mechanism, the DEMARC MUST fall back to use the TFTP file transfer mode, where the selected secure transfer mechanism in the received [URI] option (sftp/https) is replaced with the tftp.

When operating in the secure file transfer mode, the DEMARC MUST use the username (as defined in 9.1.4) to open the secure file transfer session. The DEMARC MUST use the password (as defined in 9.1.5) to open the secure file transfer session.

When a DEMARC successfully transfers a configuration file, the DEMARC SHOULD verify that the configuration file is a valid configuration file according to criteria specific to that vendor's configuration file format, syntax, contents, etc. Verification of the configuration file is not specified herein.

If the new configuration file passes the DEMARC's validation, the DEMARC SHOULD archive the current running configuration, or most recently used configuration. Such a mechanism is useful to operators to manually rollback changes if the downloaded configuration file does not work.

If a DEMARC validates the configuration file, the DEMARC MUST save the configuration file as the current or running configuration such that if the DEMARC is administratively or unintentionally rebooted, it will start up with the new configuration file running by default.

If a DEMARC validates the configuration file, the DEMARC MUST load and then run the configuration file as the current or running configuration. The process of loading a new configuration file is vendor-specific and not covered in this specification. The DEMARC MUST not require a manual or administrative reboot in order to run the configuration file. The DEMARC SHOULD load the new configuration file in such a way that traffic forwarding is unaffected on interfaces that are not changed by the new configuration.

If the new configuration file fails the validation, the DEMARC MUST validate the previously loaded configuration file.

If a DEMARC does not detect a BP-ONU or receive any LLDPDUs (see Section 8.1.2), the DEMARC MUST load the last saved configuration file.

If a DEMARC does not detect a BP-ONU and the DEMARC does not have a saved configuration file, the DEMARC MUST load a default configuration file and operate as the DEMARC would without these specifications.

9.1.4 Username for Secure File Transfer Session

The username for the secure file transfer session, established by the DEMARC with the OSS, should be one of the hardware parameters of the DEMARC, known to the OSS in advance (configured either manually or automatically by the operator) or learned during the DAC process, depending on the operator choice and provisioning strategy used in the given network.

There are multiple options for selecting the username for the secure file transfer session, such as unique device serial number, concatenation of the vendor ID and device ID, identification certificate, etc. However, these cannot be guaranteed to be globally unique and would result in additional requirements for DEMARC vendors, which might be difficult to impose. There are also backward compatibility concerns for devices already deployed, which might not support such unique identification string.

In this version of the DEMARC specification, the DEMARC MUST use the DEMARC MAC address (DEMARC chassis MAC address) as the username for the secure file transfer session. The DEMARC MUST NOT use any of the interface MAC addresses as the username for the secure file transfer session.

9.1.5 Password for Secure File Transfer Session

The password for the secure file transfer session can be any sequence of thirty-two (32) characters or less. The password should meet one or more of the following data security requirements:

1. not stored locally on the DEMARC in either clear text or encrypted form between reboots,
2. be dynamically assigned by the back office system using the challenge-response mechanism in such a way that the back office system can pre-calculate the DEMARC response in advance.

These two requirements help prevent a majority of network-based attacks, such as device identity theft, device cloning, replay attacks, etc.

In this version of the DEMARC specification, the password for the secure file transfer session is generated dynamically using the challenge-response mechanism, as defined in the following sections. The DEMARC calculates the password challenge response using a local salt (defined in the following sections) and uses the resulting password in combination with the previously established username (see Section 9.1.1 for details) to establish a session with the OSS.

9.1.5.1 Password Salt

In this version of the DEMARC specification, the DEMARC calculates the password for the secure file transfer session using its DEMARC chassis MAC address as salt, i.e., using the following equation:

PASSWORD = MD5 (CHALLENGE, DEMARC_MAC)

where CHALLENGE is the password challenge delivered to the DEMARC via a D-ONU (see Section 9.1.1 for details) using the LLDPDU (see Annex A for details), and DEMARC_MAC is the DEMARC chassis MAC address, unique for this DEMARC.

9.1.5.2 Password challenge transfer mechanism

The OSS configures each D-ONU known to be connected to a DEMARC with a password challenge, in the form of a sequence of arbitrary length. The OSS may re-provision such a password challenge on the D-ONU on the following events:

(1) discovery and registration of a D-ONU,

(2) discovery and registration (DAC) of a DEMARC connected to the given D-ONU,

(3) successful or failed configuration file transfer between the DEMARC connected to the given D-ONU and the OSS,

(4) on-demand, based on operator / network manager request, and

(5) any other reason not defined before.

This guarantees that the password challenge is used by the given DEMARC only once and the secure software download infrastructure remains immune to replay attacks and device cloning.

The 'LLDP password challenge' TLV (see Annex A for details) is transferred to the DEMARC when it is configured on the D-ONU by the OSS via eOAM, as outlined in Annex C of this specification. The D-ONU MUST NOT generate the password challenge on its own, transfer empty 'LLDP password challenge' TLVs or otherwise restart the challenge – response mechanism unless explicitly configured to do so by the OSS. The D-ONU MUST continue sending the 'LLDP password challenge' TLV(s) to the DEMARC as long as the password challenge is configured on the D-ONU. Once and only if the back office system disables the DAC function for the given D-ONU port via the eOAM per Annex C, the D-ONU MUST interrupt the transmission of the 'LLDP password challenge' TLV.

The DEMARC MUST continuously scan the incoming LLDPDUs for 'LLDP password challenge' TLV(s) and once detected, retrieves the password challenge, assembles it correctly (starting from password part number 0 towards the part number indicated in the 'Total part number' field), and uses it to calculate the current password value.

The DEMARC MUST NOT use a password challenge sequence that is incomplete (i.e., is missing any of the sequentially numbered parts) or known to be corrupt based on the [802.3] cyclic redundancy check (CRC) carried in the LLDPDU. The DEMARC supporting secure software download MUST NOT attempt to download the configuration file until a complete password challenge is received from the D-ONU and the password can be calculated.

The DEMARC supporting secure software download MUST support the two following fallback mechanisms, as defined below:

- Fallback mechanism 1: A secure file transfer session using the preferred secure file transfer mechanism (i.e., SFTP or HTTPS, as configured by the operator via the Secure File Transfer URI Option in the DHCP Offer and ACK messages sent to the DEMARC) may fail for any number of reasons. In such a case, the DEMARC MUST recalculate the password based on the received password challenge after such failure, and then wait three (3) seconds before attempting to re-establish a connection to the OSS. The DEMARC MAY attempt to establish such a connection at most four times, after which a connection failure is said to have occurred and the DEMARC will attempt to establish a session with the TFTP server, as outlined in 9.1.3.
- Fallback mechanism 2: if, by the time the DEMARC receives a DHCP Offer or ACK message from the OSS, and no 'LLDP password challenge' TLV is received from the connected ONU, the DEMARC MUST attempt to establish a session with the TFTP server, the address of which is retrieved from the Secure File Transfer URI Option carried in the DHCP Offer and Ack messages, as outlined in 9.1.3.

A DEMARC that does not support the secure file transfer protocol MUST ignore all received 'LLDP password challenge' TLV(s) and establish a session with the TFTP server in order to obtain the configuration file, using the address retrieved from the Secure File Transfer URI Option carried in the DHCP Offer and Ack messages, as outlined in 9.1.3.

9.1.5.3 Password calculation process

Once all parts of the password challenge are received by the DEMARC and the password challenge is properly assembled, the DEMARC calculates the resulting password by taking the received password challenge and the DEMARC MAC address as two parameters for the calculation listed in 9.1.2.1 of [802.1AB].

The mechanism in use by the given DEMARC type, model, or make must be known in advance to the back office, where parallel calculation takes place. The resulting MD5 hash digest represents the password to be used by the DEMARC to establish a session with the back office server. The length of the password must meet the minimum and maximum password length required by the secure file transfer protocol. If the available calculated password is larger than the password length required by the secure file transfer protocol, only the first N bytes of the calculated password are used.

9.1.6 DAC Logging

The DEMARC MUST support the capability to log event messages to a SYSLOG server.

If logging is enabled by the operator, the DEMARC MUST log each attempt to connect to the OSS storing the DEMARC configuration files to the SYSLOG server, local storage or both. The DEMARC MUST log a successful connection to OSS. The DEMARC MUST log to the SYSLOG server each attempt to transfer a file from such a server. The DEMARC MUST log to the SYSLOG server a successful configuration file transfer. The DEMARC MUST log to the SYSLOG server the result of a configuration file validation, if such an optional validation process is performed.

9.2 D-ONU Requirements for DAC

All D-ONUs compliant with DPoE version 1.0 specifications MUST support DAC.

The D-ONU MUST implement [802.1AB] LLDP Transmitter and Receiver agents.

The D-ONU MUST transmit the DPoE LLDPDU with a source address of the D-ONU EPON MAC address.

The D-ONU MUST transmit the LLDPDU to any of the destination MAC addresses specified in [802.1AB] Clause 7.1, Table 7-1. The D-ONU MAY transmit the LLDPDU to any of the reserved MAC addresses specified in [802.1d], Table 7-10.

The D-ONU LLDPDU transmission is a LLDPDU as defined in [802.1AB], section 9.1.2.

The D-ONU LLDPDU MUST include the [802.1AB] mandatory TLVs required in [802.1AB], section 9.1.2.1, and specified in [802.1AB], section 8.2. The D-ONU MUST transmit TLV 0x7F in the LLDPDU as specified in Annex A, on all MI interfaces configured to support DAC. The D-ONU MUST ensure the interval between PDU transmissions complies with section 9.1.1 in [802.1AB]. The D-ONU LLDPDU MUST be in a direct-encoded LLDP format. The D-ONU LLDPDU frame header MUST NOT contain any [802.1Q], or [802.1AE] headers or tags as specified in [802.1AB]. The D-ONU LLDPDU MUST NOT be encrypted or encapsulated in any way.

A single D-ONU UNI interface MAY be connected to, at most, one DEMARC. Cascading DEMARC devices on a single UNI port in any configuration is not supported by this specification.

The D-ONU must support the eOAM messages defined in Annex C of this specification.

9.3 DPoE System Requirements for DAC

The DPoE System MUST provide a DHCP Relay Agent to relay DHCP broadcast messages from a DEMARC to a DHCP server.

The DPoE System MUST provide means to configure multiple DHCP servers specifically for the DAC DHCP Relay Agent, as defined in Annex D (see DAC DHCP Relay Agent Configuration).

DEMARC IP management unicast services are built with E-LINE (EPL) terminating at the DPoE System. Each DEMARC Serving Group (DAC-SG[3]) may consist of one or more S-VIDs with each DEMARC being assigned a single C-VID. Thus the encapsulation for the management EVC would consist of a dynamically assigned S-VID and C-VID based on the DAC-SG configuration specified in Annex D. Requirements for configuring DAC-SG are specified in Annex D.

All the requirements for the DPoE System related to DHCP and DAC can be found in Annex D.2.

The DPoE System MUST configure a dedicated management Logical Link Identifier (LLID) and corresponding classifiers for the given D-ONU MI when the vCM receives a configuration file with the TLV 43.5.16 (as defined in Annex B) indicating the MI is configured to operate with a DEMARC. The D-ONU MUST use the management LLID to transfer DEMARC management-related traffic from the D-ONU to the DPoE System. The DPoE System MUST use the management LLID to transfer DEMARC management traffic from the DPoE System to the D-ONU.

When multiple DEMARCs are connected to a D-ONU, the DPoE System MUST configure the D-ONU to use the management LLID to forward management traffic from all DEMARCs to the OSS. In other words, a single LLID is used for all DEMARC management traffic. In such a case, the DPoE System MUST NOT allocate additional management LLIDs for such a D-ONU. The configuration process in this case is similar to the one listed above, remembering that the S-Tag + C-Tag combination for the new DEMARC is different from the other DEMARC.

The DPoE System MUST support the eOAM messages defined in Annex C of this specification.

The DPoE System MUST support the IPNE configuration requirements defined in Annex D of this specification.

[3] Please see DPoE-IPNEv1.0 for the definition and specific requirements for DAC-SG.

9.4 Configuration Requirements

DEMARC Auto Configuration (DAC) Enable/Disable Configuration (TLV 43.5.16, as defined in Annex B) provides a mechanism to enable/disable the DAC operation of the D-ONU port(s) that associate with the Metro Ethernet services, as listed in Annex B. For D-ONU ports associated with the EPL service (through CMIM, TLV 43.5.4), DAC Enable/Disable controls the DAC operation of the given port(s). By default, DAC is disabled.

Annex A LLDPDU for DPoE

The D-ONU MUST transmit an LLDPDU with:

CableLabs OUI (0x001000)

TLV type 0x7F

TLV Length is variable depending on which optional fields are included.

Length = 4 bytes + X where X is the length of the 'information string'

The 'information string' is the DPoE-specific parameters.

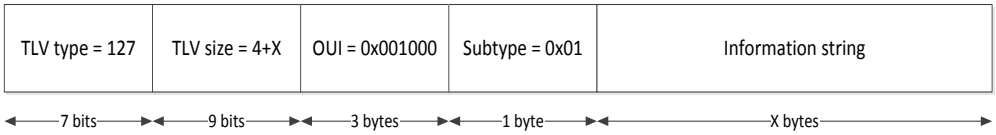

Figure 9 - DPoE-specific LLDPDU Structure

Table 8 below indicates the required and optional values for the D-ONU and DEMARC LLDPDU for DPoE. Other Subtype values are reserved for future use.

Table 8 - LLDPDU Vendor-specific (TLV 127) for DPoE with OUI (0x00-10-00)

Name	Type	Subtype	Length (bytes)	Value	Value Range (Int)
LLDP DPoE Version	127	1	2	2 0	na
	DPoE Version (major)		1	2	0...15
	DPoE Version (minor)		1	0	0…15
LLDP DPoE Bridge Configuration	127	2	25	See below	See below
	Bridge Sub-Type		1	0 = [802.1ad] 1 = [802.1ah] I-Tag Only + B-DA 2 = [802.1ah] I-Tag + B-Tag + B-DA	0…2 3…15 (reserved)
	S-Tag		4	DPoE System assigned S-Tag for in-band DEMARC management from DPoE System through D-ONU to DEMARC	
	C-Tag		4	DPoE System assigned C-Tag for in-band DEMARC management from DPoE System through D-ONU to DEMARC	
	I-Tag		6	DPoE System assigned I-Tag	
	B-Tag		4	DPoE System assigned B-Tag	
	B-DA		6	DPoE System assigned B-DA for destination station	
LLDP password challenge	127	255	Varies[a)]	Part k of N of the password challenge. This field is further divided into the fields, as specified below:	
	Part number[b)]		2	Actual part number (1 byte) Total part number (1 byte)	
	Part payload[c)]		Max 505		

Table 8 Notes

a) The configured password challenge of arbitrary length may be divided into a number of parts, each with the maximum size of 507 bytes, where a single TLV may transfer only one part of the password challenge. The selection of the actual size of the TLV is implementation-dependent and does not need to be regulated in any way as long as the maximum TLV size is observed. The last part of the password challenge may be smaller than 507 bytes as indicated by the TLV size field.

For example, if the password challenge is 1100 bytes long, three 'LLDP password challenge' TLVs will be used to transfer this password challenge to the DEMARC: the first TLV with 505 bytes of payload, the second TLV with 505 bytes of payload, and the third TLV with 1100 – 505 – 505 = 90 bytes of payload. The size of individual TLVs is indicated in the 'TLV size' field by adding the size of the 'Part payload' field and the size of the 'Part number' field.

In this case, all TLVs will fit into a single LLDPDU (total size smaller than 1500 bytes). It is allowed for the TLVs to transfer in different LLDPDUs, if needed. In this case, the transmission of the password challenge spans multiple LLDPDUs in a sequential manner, i.e., it is restarted only when a complete password challenge is transferred to the DEMARC.

b) The 'Part number' field may indicate the sequential number of the password challenge part that is being transferred in the given TLV. This field comprises two subfields, i.e., 'Actual part number' (1 byte) indicating the number of the current password challenge part and 'Total part number' (1 byte) indicating how many parts there are in the password challenge in total.

   The numbering starts from 0 and continues until all parts of the password challenge are transferred to the DEMARC, each in a dedicated TLV. This part number allows the DEMARC to properly concatenate individual parts of the password challenge sequence. It also allows the DEMARC to discard any incomplete password challenge sequences should the numbering carried in the 'Part number' be discontinuous in any manner, i.e., one or more parts of the password challenge were missing.

   At most, 255 parts of a password challenge may be transferred between the D-ONU and the DEMARC, limiting effectively the length of the password challenge to 255 * 505 = 128775 bytes. This maximum length is considered sufficient to support any existing challenge – response mechanisms with the MD5 hash.

c) The 'Part payload' is the TLV section that carries the actual fragment of the password challenge, with the maximum length of 505 bytes and the minimum length of 1 byte. The D-ONU LLDP Transmit agent MUST NOT transfer the 'LLDP password challenge' TLV if the 'Part payload' size is equal to zero.

Annex B CM Configuration File TLVs for LLDP

B.1 DAC Disable/Enable Configuration

This parameter defines the DAC administrative configuration of the D-ONU port (s) associated with the MEF service. For the D-ONU port associated with the MEF EPL service, this parameter controls the DAC for the given port.

This TLV can be configured with value 0 or 1, where 0 is for Disabling the DAC, and 1 is for Enabling the DAC. Without specifying this TLV, the DAC is disabled by default.

SubType	Length	Value
43.5.16	1	1 or 0

Annex C L-OAMPDUs for LLDP

This annex contains attributes to support DEMARC devices subtended from a D-ONU.

C.1 DAC Configuration Parameters (0xD7/0x0800)

Objects: User Port

This attribute represents a set of DAC-related configuration parameters associated with the LLDP Transmit/Receive agent operating on the given UNI port, i.e., the aggregate of S-Tag, C-Tag, I-Tag, B-Tag, and B-DA in whatever combination that needs to be relayed by the LLDP to the DEMARC. This attribute must be associated with the User Port Object.

Table 9 - DAC Configuration Parameters

Size	Name	Description
4	S-Tag	S-Tag value for DAC management traffic
4	C-Tag	C-Tag value for DAC management traffic
6	I-Tag	I-Tag value for DAC management traffic
4	B-Tag	B-Tag value for DAC management traffic
6	B-DA	B-DA value for DAC management traffic

C.2 DAC Configuration Flags (0xD7/0x0801)

Objects: User Port

This attribute indicates which of the DAC Configuration Parameters listed in 0xD7/0x0800 are to be processed by the DAC function on the given port (corresponding bit is set to 1) or not (corresponding bit is set to 0).

Table 10 - DAC Configuration Flags

Size	Name	Description
1	DAC Configuration Flags	Bit-encoded field, indicating which of the DAC Configuration Parameters listed in 0xd7/0x0800 are to processed by DAC function on the given port (corresponding bit is set to 1) or not (corresponding bit is set to 0). The following bit encoding is defined. bit 0: S-Tag bit 1: C-Tag bit 2: I-Tag bit 3: B-Tag bit 4: B-DA bits 5-7 are reserved and set to 0.

C.3 DAC Password Challenge (0xD7/0x0802)

Objects: User Port

This attribute sets the password challenge for the given DAC instance, required for the operation of the DAC mechanism and secure config file download mechanism via SFTP/HTTPS, as defined in DEMARC. The password challenge may be set for each LLDP Transmit/Receive agent operating on the given UNI port and can be modified independently of the S-Tag and C-Tag configuration parameters. The vCM MUST associate this attribute with the User Port Object.

Table 11 - DAC Password Challenge

Size	Type	Name	Description
Varies	String	password challenge string	Password challenge for the secure config file download, as defined in DEMARC

C.4 DAC Configuration Enable / Disable (0xD7/0x0803)

Objects: User Port

This attribute is used to control the admin status of the given LLDP instance associated with the specific User Port Object. When set to '1', the given LLDP instance is enabled, while when set to '0', the given LLDP instance is disabled. When read as '1', the given LLDP instance is currently enabled, while when read as '0', the given LLDP instance is currently disabled. By default, this attribute is assigned the value of '0'" upon D-ONU reboot.

This attribute must be associated with the User Port Object.

Table 12 - DAC Configuration Enable / Disable

Size	Description	Units	Default	Min	Max
1	LLDP instance status	Boolean	0	0	1

Annex D IP Network Element Configuration Requirements

D.1 Serving Groups

DPoE Systems use [802.1Q] S-VLANs and stacked VLANs (S-VLAN and C-VLAN) to forward Ethernet frames carrying IP and ethernet traffic for DEMARC auto-configuration traffic as defined in this specification.

The DPoE System MUST have a set of commands to configure the allocated S-VIDs for the purpose of dynamically generating the classification or classification and encapsulation values used on the D-ONU and DPoE System.

These dynamically generated S-VID or S- and C-VIDs are used in lieu of explicit classification or classification and encapsulation values set in the CM configuration file.

An operator could configure a bundle and then associate that bundle with an SG, which would indicate which S-VLANs were allocated to the given SG. In fact, an operator could associate the same bundle with multiple SGs for differing purposes. As an example, an operator could configure a bundle including all TUs on the DPoE System and then proceed to associate that bundle with an SG for IP(HSD), another SG for eMTA services, and a third SG for DAC.

Below is an example of the configuration of a bundle with an associated SG for that bundle.

```
Sg bundle 1
Description
!
interface TUL 0
sg bundle 1

!
Sg DAC
   Sg bundle 1
   s-vlan 1004
   polling-type BE
   upstream rate 100kbps
   downstream rate 100kbps
   match DAC-TLV
!
```

Example format of a command for S-VLAN configuration at the CLI or in a configuration file:

```
s-vlan N
```

Where N is a set of S-VIDs, each between 0 to 4095 expressed as a positive integer.

In this example once the SG HSD was configured, the DPoE System would instantiate an interface for the SG, which could be used as an SG IP interface as described below. Each defined SG would have match conditions to associate the service elements in the configuration file to the correct pool of S-VIDs.

The match conditions utilized for the SG object must look at the CM configuration file per upstream and downstream service flow pair.

To match on an SF for DAC, the vCM MUST be able to parse on the presence of the DAC Disable/Enable Configuration TLV and allocate an S,C from the S-VID pool associated with the matched SG.

The vCM MUST also allocate the QoS parameters associated with the SG when there are no explicit and supported QoS parameters associated with the service-flow.

When the vCM provisions a transport-mode MI for DEMARC auto-configuration, the vCM MUST utilize the polling type and the configured rate associated with the SG for DAC to configure the QoS parameters for the service flow.

The DPoE System MUST have a configuration element for QoS parameters associated with a given SG to include the following variables:

- Polling-type: RTPS or best effort.
- Upstream Rate: (in kbps).
- Downstream Rate: (in kbps).

A DPoE System MUST be able to associate multiple serving groups to the same bundle.

A DPoE System MUST allow the allocation of a set of S-VIDs for use within an individual SG.

The DPoE System MUST provide both a CLI command and a configuration file command to configure one or more S-VLANs to an SG.

D.1.1 Example IP-SG Configuration for DAC

The IP-SG for DAC is just another example of the flexibility intended in the IP-SG models. The example configuration for an IP-SG for DAC is shown below:

```
Sg bundle 1
Description
!
interface TUL 0
sg bundle 1
!
interface TUL 1
sg bundle 1

Sg DAC
   Sg bundle 1
   s-vlan 1005
   polling-type BE
   upstream rate 100kbps
   downstream rate 100kbps
   match DAC-TLV
!
interface Sg DAC
! Example DAC IP Network
   ip address 10.200.205.1 255.255.255.0
   ipv6 address 2001:db8:5:1/64
   ip access-list 500 in
   ip access-list 501 out
   dhcp address 10.1.1.1
   Dac file-transfer
       Method [SFTP | HTTPS]
       Server [IPV4 | IPV6] [HOST]
```

D.2 DAC DHCP Relay Requirements

The DPoE System (acting as a DHCP relay-agent) MUST insert the CMTS DOCSIS Version Number option and DPoE System Version Number option as described in [CANN-DHCP-Reg] into all DEMARC DHCP messages relayed from the DEMARC to the DHCP servers (configured as part of the DAC-SG). These are the same option code TLVs used for a vCM and defined in [DPoE-MULPIv1.0].

Additionally, the DPoE System is responsible for receiving DHCP Offer and Ack messages from the OSS destined for a DEMARC and if configured appropriately by the operator, insure that the DHCP Offer and Ack messages contain a Secure File Transfer URI Option. Identification of whether the given DHCP Offer or ACK messages are addressed to a DEMARC is vendor-specific and outside the scope of this specification. In one example, the DPoE System might keep track of the DEMARC MAC addresses, retrieved from the upstream DHCP Request messages, identified based on the specific IP address pool. The Secure File Transfer URI Option provides the Uniform Resource Identifier (URI) for the location where the target DEMARC configuration file is stored, together with the

indication of the preferred secure file transfer mechanism that the DEMARC is requested to use to retrieve the configuration file.

When the Secure File Transfer URI Option is not present in the DHCP Offer or Ack message received from the OSS, and if the DPoE System is configured to do so, the DPoE System MUST add the Secure File Transfer URI Option into the DHCP Offer and Ack message before forwarding the DHCP Offer or Ack message to the DEMARC. When a DPoE System's IP-SG is configured with a DAC file transfer method and the DPoE System receives a DHCP Offer message that includes the DHCP Option 66 as defined in [RFC2132], and does not include the Secure File Transfer URI Option, the DPoE System MUST insert the Secure File Transfer URI Option to the DHCP Offer or Ack message before forwarding the DHCP Offer or Ack message to the DEMARC.

The URI is constructed with the standard form as defined in [RFC3986]:

foo://example.com:8042/over/there?name=ferret#nose'

For the purpose of the DPoE System file transfer method, the URI reference used is [METHOD]://[HOST]/[BOOTFILE]].

To construct the URI sent in the Secure File Transfer URI Option, the DPoE System MUST use the following values to create the URI from both the DPoE System Local configuration and the TFTP options present in the original DHCP Offer message:

- The DPoE System MUST use the method identified in the DAC file transfer proxy object defined in the configuration of the DPoE System as the [METHOD] section of the URI. Two values are possible in here i.e. SFTP and HTTPS.
- The DPoE System MUST use the configured host value [HOST] under the DAC file transfer object, if configured. If the configured host value under the DAC file transfer object is not configured, the DPoE System MUST use the valid fields after the length field within DHCP Option 66 as the [HOST] section of the URI.
- The [BOOTFILE] is populated based on the bootfile field in the DHCP Offer or Ack message.

The DPoE System MUST only add a single instance of the Secure File Transfer URI Option to a single DHCP Offer or Ack message. The DPoE System MUST support HTTPS as a DAC file transfer method within the DAC file transfer object. The DPoE System MUST support SFTP as a DAC file transfer method within the DAC file transfer object. The DPoE System MUST support the configuration of a host under the DAC file transfer object. The DPoE System MUST NOT support the configuration of multiple DAC file transfer methods within a single IP-SG. Different IP-SGs MAY have different DAC file transfer mechanisms defined. If the DAC file transfer server is configured for an FQDN, the DPoE System MUST perform DNS resolution prior to insertion into the Secure File Transfer URI Option . The DPoE System SHOULD cache the DNS response for the file transfer server up to the advertised TTL.

An example of the configurable options of the DAC file transfer object

```
dac file-transfer
   method [SFTP|HTTPS]
   server [ipv4] x.x.x.x [or] FQDN
```

The DAC file transfer object can be independently configured for each DAC-SG.

Appendix I Acknowledgements

On behalf of our industry, we would like to thank the following individuals for their contributions to the development of this specification.

Contributor	Company Affiliation
John Dickinson, Edwin Mallette	Bright House Networks
Paul Gray, Victor Hou	Broadcom
Curtis Knittle	CableLabs
Jimmy Hu	Ciena
Tim Brophy	Cisco Systems
Mehmet Toy, Shamim Akhtar	Comcast
Mike Holmes, Wen Li, Jianhui Zhou, Fulin Pan	Finisar
Victor Blake	Independent Consultant
Robert Harris, Kevin A. Noll, Armin Sepehri	Time Warner Cable
Marek Hajduczenia, Nevin Jones	ZTE