Society of Cable Telecommunications Engineers

ENGINEERING COMMITTEE
Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 79-3 2017

DOCSIS 2.0 + IPv6 Cable Modem Standard

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards and Operational Practices (hereafter called "documents") are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE members.

SCTE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE web site at http://www.scte.org.

140 Philips Road
Exton, PA 19341

Contents

List of Tables

1 SCOPE

1.1 Scope and Purpose

This document is an extension to the DOCSIS 2.0 family of standards, which define high-speed data-over-cable systems. For an overview of DOCSIS 2.0, refer to [RFIv2.0]. The [RFIv2.0] specification requires the CM to support IP version 4 for provisioning and management. This present document provides IPv6 provisioning and management functionality for DOCSIS 2.0 CMs, connected IPv6 eSAFEs, and external CPE devices. The term DOCSIS 2.0+IPv6 CM is used to represent such Cable Modems.

This specification identifies a relevant sub-set of requirements from [MULPIv3.0], which, when implemented on a DOCSIS 2.0 CM, allow for IPv6 provisioning and management.

IPv6 provisioning of CMs using DHCPv6 has been defined in [MULPIv3.0], including the implementation of DHCPv6 host functionality. This specification relies on such requirements specified in MULPIv3.0, and provides needed modifications to accommodate them on a DOCSIS 2.0+IPv6 CM.

IPv6 management of CMs using SNMPv2c has been defined in [MULPIv3.0] and [OSSIv3.0]; this specification provides a sub-set of those requirements which are required to manage a DOCSIS 2.0+IPv6 CM via IPv6.

IPv6 Link-Local Multicast is required for provisioning of an IPv6 Host. This specification defines additional requirements for processing of IPv6 Link-Local Multicast packets within a DOCSIS 2.0+IPv6 CM to enable its provisioning and the provisioning of eSAFEs and external CPEs.

1.2 Conventions

In this document it is assumed that the CM complies with the [RFIv2.0] specification for all behaviors not specified in this specification.

As in [MULPIv3.0], the term "CPE" includes both externally connected CPE devices and eSAFEs. The term "CMCI port" describes physical interfaces to which externally connected CPE devices can attach. The term "Logical CPE Interface" refers to an interface between the CM and an eSAFE. The term "CPE interface" refers to an interface that is either a CMCI port or a Logical CPE Interface.

1.3 Requirements

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

"MUST"	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

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

2 REFERENCES

2.1 Normative References

The following documents contain provisions, which, through reference in this text, constitute provisions of this document. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision; and while parties to any agreement based on this document are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1.1 Normative References

[MULPIv3.0]	ANSI/SCTE 135-2 2013, DOCSIS 3.0 Part 2: MAC and Upper Layer Protocols.
[OSSIv2.0]	ANSI/SCTE 79-2 2016, DOCSIS 2.0 Operations Support System Interface.
[OSSIv3.0]	ANSI/SCTE 135-4 2013, DOCSIS 3.0 Part 4: Operations Support Systems Interface.
[RFIv2.0]	ANSI/SCTE 79-1 2016, DOCSIS 2.0 Part 1: Radio Frequency Interface.
[CANN-DHCP-Reg]	CL-SP-CANN-DHCP-Reg-I05-110623, June 23, 2011, Cable Television Laboratories, Inc.
[RFC 2013]	IETF RFC 2013, RFC SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2, November 1996.
[RFC 3419]	IETF RFC 3419, Textual Conventions for Transport Addresses, December 2002.
[RFC 4113]	IETF RFC 4113, Management Information Base for the User Datagram Protocol (UDP), June 2005.
[RFC 4293]	IETF RFC 4293, Management Information Base for the Internet Protocol (IP), April 2006.
[RFC 4639]	IETF RFC 4639, Cable Device Management Information Base for Data-Over-Cable Service Interface Specification (DOCSIS) Compliant Cable Modems and Cable Modem Termination Systems, December 2006.

2.2 Informative References

The following documents might provide valuable information to the reader but are not required when complying with this document.

[SECv3.0]	ANSI/SCTE 135-3 2013, DOCSIS 3.0 Part 4: Security Services.
[RFIv1.1]	ANSI/SCTE 23-1 2010, DOCSIS 1.1 Part 1: Radio Frequency Interface.
[RFC 2132]	IETF RFC 2132, DHCP Options, and BOOTP Vendor Extensions, March 1997.
[RFC 2462]	IETF RFC 2462, IPv6 Stateless Address Autoconfiguration, December 1998.
[RFC 2710]	IETF RFC 2710, Multicast Listener Discovery (MLD) for IPv6, October 1999.

[RFC 2933] IETF RFC 2933, Internet Group Management Protocol MIB, October 2000.

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

[RFC 3513] IETF RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture, April 2003.

[RFC 4291] IETF RFC 4291, IP Version 6 Addressing Architecture, February 2006.

[RFC 4323] IETF RFC 4323, Data Over Cable System Interface Specification Quality of Service Management Information Base (DOCSIS-QoS MIB), January 2006.

[RFC 4361] IETF RFC 4361, Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4), February 2006.

[RFC 4605] IETF RFC 4605, Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding (IGMP/MLD Proxying), August 2006.

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
- 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
- Internet Engineering Task Force (IETF), Internet: http://www.ietf.org/

3 TERMS AND DEFINITIONS

This document defines the following terms and definitions:

DOCSIS 2.0+IPv6 CM A DOCSIS 2.0 Cable Modem that supports IPv6 Provisioning and Management and supports connected IPv6 eSAFEs and external CPE devices.

4 ABBREVIATIONS

This document uses the following abbreviations:

APM	Alternate Provisioning Mode
CPE	Customer Premises Equipment
DPM	Dual-Stack Provisioning Mode
EAE	Early Authentication and Encryption
DSID	Downstream Service Identifier
GMAC	Group Media Access Control
LAN	Local Area Network
MDD	MAC Domain Descriptor
MDF	Multicast DSID Forwarding
MIB	Management Information Base
SNMP	Simple Network Management Protocol

5 CM INITIALIZATION

5.1 DOCSIS Initialization

5.1.1 EAE

The DOCSIS 2.0+IPv6 CM is not required to support Early Authentication and Encryption (EAE) per the Early Authentication and Encryption (EAE) section of [SECv3.0]. Because these CMs are not expected to support EAE, the recommended CMTS EAE enforcement configuration should be to enforce EAE via Policy 1 (No EAE Enforcement), Policy 2 (Ranging-based EAE Enforcement), or Policy 3 (Capability-based Enforcement). If EAE is enabled at the CMTS, and the CMTS is configured to enforce EAE via Policy 4 (Total EAE Enforcement), the DOCSIS 2.0+IPv6 CM will not be able to register.

5.1.2 MDD Processing

As with DOCSIS 3.0, the DOCSIS 2.0+IPv6 CM MUST look for the presence of the DOCSIS 3.0 MAC Domain Descriptor (MDD) message (see MAC Domain Descriptor section of [MULPIv3.0]) on the downstream channel it has acquired during downstream scanning and synchronization. Because the MDD message may be fragmented when a MAC domain is complex, the DOCSIS 2.0+IPv6 CM MUST parse the fragments of the MDD message. The DOCSIS 2.0+IPv6 CM looks for the IP Provisioning TLV (TLV 5), and optionally for the DSG DA-to-DSID Association Entry TLV (TLV 13).

The IP provisioning mode is communicated in the IP Provisioning Mode TLV (TLV 5.1) as defined in the IP Initialization Parameters TLV section of [MULPIv3.0]. The DOCSIS 2.0+IPv6 CM MUST support single stack IPv4 and single stack IPv6 operation. The DOCSIS 2.0+IPv6 CM MAY support Alternate Provisioning mode and/or Dual Stack Provisioning mode. The DOCSIS 2.0+IPv6 CM MUST support the IP Provisioning Mode Override. Refer to[MULPIv3.0] and [OSSIv3.0] for details of the IP Provisioning Mode Override feature.

If the DOCSIS 2.0+IPv6 CM is capable of GMAC Explicit Multicast DSID Forwarding, the DOCSIS 2.0+IPv6 CM MUST utilize the Pre-Registration DSID (TLV 5.2) communicated in the MDD message. Additionally, if the DOCSIS 2.0+IPv6 CM that supports GMAC Explicit Multicast DSID Forwarding is an eCM with an eSTB, the CM MUST utilize the DSG DA-to-DSID Association Entry TLV (TLV 13) as defined in the DSG DA-to-DSID Association Entry section of [MULPIv3.0] to learn the DSID(s) associated with DSG tunnel(s).

5.2 IP Initialization

5.2.1 Establishing IP Connectivity

The DOCSIS 2.0+IPv6 CM determines the IP provisioning mode via the CmMdCfg management object defined in [OSSIv3.0]. The CM MUST support the following configurable IP Provisioning Mode Override policies:

- Honor MDD: the CM determines the IP provisioning mode by the IP Provisioning Mode TLVs in the MDD message, or by the absence of the MDD message. This is the default behavior.
- IPv4 only: CM will acquire a single IPv4 address for the CM management stack, overriding the TLVs in the MDD message.
- IPv6 only: CM will acquire a single IPv6 address for the CM management stack, overriding the TLVs in the MDD message.

If the DOCSIS 2.0+IPv6 CM does not receive an MDD from the CMTS, the DOCSIS 2.0+IPv6 CM MUST perform IPv4 provisioning as defined in the CM Configuration Interface Specification Annex section of [RFIv2.0]. The MDD IP Provisioning Mode TLV signals to the DOCSIS 2.0+IPv6 CM one the following four IP provisioning modes:

- IPv4 Only
- IPv6 Only
- Alternate Provisioning Mode (APM)
- Dual-stack Provisioning Mode (DPM)

If the MDD IP Provisioning Mode TLV signals IPv4 Only provisioning, the DOCSIS 2.0+IPv6 CM MUST perform IPv4 provisioning as defined in [RFIv2.0]. If the MDD IP Provisioning Mode TLV signals IPv6-Only provisioning, the DOCSIS 2.0+IPv6 CM MUST perform IPv6 Only provisioning as defined in the Establishing IP Connectivity section of [MULPIv3.0].

The DOCSIS 2.0+IPv6 CM MAY implement APM. If the CM does not implement APM and the MDD IP Provisioning Mode TLV signals APM, the DOCSIS 2.0+IPv6 CM SHOULD default to either IPv4 Only or IPv6 Only provisioning. Defaulting to IPv4 Only provisioning is recommended. If the DOCSIS 2.0+IPv6 CM optionally implements APM, it MUST do so as defined in the Establishing IP Connectivity and the Alternate Provisioning Mode (APM) Operation sections of [MULPIv3.0], with the exception that IPv4 provisioning is done per [RFIv2.0].

The DOCSIS 2.0+IPv6 CM MAY implement DPM. If the CM does not implement DPM and the MDD IP Provisioning Mode TLV signals DPM, the DOCSIS 2.0+IPv6 CM SHOULD default to either IPv4 Only provisioning, IPv6 Only provisioning, or APM. Defaulting to IPv4 Only provisioning is recommended. If DOCSIS 2.0+IPv6 CM optionally implements DPM, it MUST do so as defined in the Establishing IP Connectivity and the Dual-stack Provisioning Mode (DPM) sections of [MULPIv3.0], with the exception that IPv4 provisioning is done per [RFIv2.0].

MULPIv3.0 specifies the use of the DHCPv6-style client identifier for DHCPv4 [RFC 4361], while RFIv2.0 assumes the DHCPv4 client will use a client identifier as specified in section 9.14 of [RFC 2132]. Therefore, any management application that correlates the DHCPv4 identifier and the DHCPv6 identifier for a CM will need to be aware of the different DHCPv4 client identifier formats, and use a different correlation computation for a CM provisioned according to this specification.

5.2.2 Establish IPv4 Network Connectivity

The DOCSIS 2.0+IPv6 CM MUST establish IPv4 connectivity using DHCPv4 as defined in the "Establish IP Connectivity" and the "DHCP Fields Used by the CM" sections of [RFIv2.0]. During DHCPv4 renew and rebind operations, the DOCSIS 2.0+IPv6 CM processes DHCPACK messages and behaves as defined in the "DHCP Fields Used by the CM" Annex section of [RFIv2.0].

5.2.3 Establish IPv6 Network Connectivity

The DOCSIS 2.0+IPv6 CM MUST establish IPv6 connectivity as defined in the Establish IPv6 Network Connectivity section and associated subsections of [MULPIv3.0]. During DHCPv6 renew and rebind operations, the DOCSIS 2.0+IPv6 CM processes DHCPv6 Reply messages and behaves as defined in the DHCPv6 Renew Fields Used by the CM section of [MULPIv3.0].

5.2.4 Establish Time of Day

When operating in IPv4 mode, the DOCSIS 2.0+IPv6 CM MUST establish date and time as defined in the Establish Time of Day section of [RFIv2.0]. When operating in IPv6 mode, the DOCSIS 2.0+IPv6 CM MUST establish date and time in a similar manner, as defined in the Establish Time of Day section of [RFIv2.0], but utilizing IPv6 as the Network Protocol by learning the server address from the Time Protocol Servers sub-option [CANN-DHCP-Reg].

5.2.5 Transfer Operational Parameters

The DOCSIS 2.0+IPv6 CM MUST download a configuration file using TFTP as defined in [RFIv2.0] when using IPv4 as the network protocol. The DOCSIS 2.0+IPv6 CM MUST download a configuration file using TFTP as defined in [RFIv2.0] when using IPv6 as the network protocol. When it uses IPv6 as the network protocol, the 2.0+IPv6 CM has the option to select only the first TFTP server address listed in the DHCPv6 TFTP Server Addresses option. The DOCSIS 2.0+IPv6 CM MUST support the TLV "TFTP Server Provisioned Modem IPv6 Address" (TLV 59).

If the DOCSIS 2.0+IPv6 CM receives an ICMP Destination Unreachable message for the current TFTP server at any time during the configuration file download process, the DOCSIS 2.0+IPv6 CM MUST terminate the configuration file download on the TFTP server whose address is included in the ICMP Destination Unreachable message without performing the TFTP Request Retries or the TFTP Download Retries [RFIv2.0].

5.3 Modem Capabilities and Vendor Class Reporting

The DOCSIS 2.0+IPv6 CM MUST include the modem capabilities in the DHCP messages (Modem Capabilities encodings) as defined in [RFIv2.0] and the DHCP messages as defined in [MULPIv3.0] with the following exceptions listed below. The DOCSIS 2.0+IPv6 CM MUST include modem capabilities in Registration Request messages as defined in [RFIv2.0].

A DOCSIS 2.0+IPv6 CM MUST report a DOCSIS Version (TLV 5.2) of DOCSIS v2.0 in all interactions with provisioning servers and Registration Request messages transmitted to the CMTS. The DOCSIS 2.0+IPv6 CM MUST include the following capability encodings from [MULPIv3.0]:

- Multicast DSID Support (TLV 5.32)
- Multicast DSID Forwarding (TLV5.33)
- Frame Control Type Forwarding (TLV 5.34)
- IPv6 Support (TLV 5.39) = 1

If the DOCSIS 2.0+IPv6 CM supports Upstream Drop Classifier Functionality (see Filtering IPv6 Traffic [MULPIv3.0]), it MUST report the Upstream Drop Classifier Support capability (TLV 5.38) in the Modem Capabilities encodings of the DHCP and Registration Request messages.

The values reported in these capabilities depend on the type of IPv6 support provided by the DOCSIS 2.0+IPv6 CM, and are described in the GMAC Explicit DSID Forwarding, IPv6 Multicast for MDF Incapable CMs, and Filtering IPv6 Traffic sections of this document.

The capabilities are carried in DHCPv4 messages as defined in [RFIv2.0] and in DHCPv6 messages as defined in [MULPIv3.0].

A DOCSIS 2.0+IPv6 CM MUST report "docsis2.0:xxxxxxx" in the DHCPv4 Vendor Class Identifier option per [RFIv2.0].

A DOCSIS 2.0+IPv6 CM MUST report DHCPv6 Vendor Class option containing 32-bit number 4491 (the Cable Television Laboratories, Inc. enterprise number) and the string "docsis2.0".

5.4 CM Registration

The DOCSIS 2.0+IPv6 CM is required to register with both DOCSIS 3.0 and pre-DOCSIS 3.0 CMTS platforms. When the DOCSIS 2.0+IPv6 CM registers with a DOCSIS 2.0 CMTS, registration follows [RFIv2.0]. When a DOCSIS 2.0+IPv6 CM registers with a DOCSIS 3.0 CMTS, registration may follow either [RFIv2.0] or

[MULPIv3.0]. When a large number of TLV IPv6 classifiers and UDC encodings are included in the configuration file, the DOCSIS 2.0+IPv6 CM can reach the REG-REQ/REG-RSP size limit of 1500 bytes imposed by [RFIv2.0], causing registration to fail. As a result, the DOCSIS 2.0+IPv6 CM needs to support the ability to use the registration message fragmentation methods defined in [MULPIv3.0] when registering with a DOCSIS 3.0 CMTS.

The DOCSIS2.0+IPv6 CM MUST perform registration using REG-REQ message if the CM does not receive an MDD from the CMTS. A DOCSIS 2.0+IPv6 CM MUST NOT send a REG-REQ-MP message when the CM has not received an MDD on its primary Downstream Channel. The DOCSIS2.0+IPv6 CM MUST perform registration using the REG-REQ-MP message when the CM has received an MDD on its primary Downstream Channel. The DOCSIS2.0+IPv6 CM MUST process and acknowledge a REG-RSP-MP message received from the CMTS whenever it has previously sent a REG-REQ-MP message.

5.5 TLV Encodings

The DOCSIS 2.0+IPv6 CM supports the TLV encodings defined in [RFIv2.0]. The DOCSIS 2.0+IPv6 CM additionally supports the TLV encodings defined in [MULPIv3.0] that are described in this document.

6 IPV6 TRAFFIC

6.1 Multicast handling

Devices on an IPv6 network communicate using several well-known multicast addresses per [RFC 4291].

Prior to registration, a DOCSIS 2.0+IPv6 CM is required to forward packets addressed to certain well-known multicast addresses to its IP stack. The well-known IPv6 Addresses include the IPv6 Link Local Scope All Nodes Address (33-33-00-00-00-01, FF02::1) and the Solicited Node Addresses. The DOCSIS 2.0+IPv6 CM calculates the Link Local Solicited Node Address (33-33-ff-xx-xx-xx, FF02:0:0:0:0:1:FFxx:xxxx) based on its MAC address per [RFC 3513]. The DOCSIS 2.0+IPv6 CM sends MLDv1 join messages for its solicited node multicast addresses for both the calculated link-local address and the MSO assigned global IPv6 address.

The DOCSIS 2.0+IPv6 CM is required to forward the multicast traffic necessary for IPv6 CPE provisioning. This traffic includes the well-known IPv6 multicast traffic addressed to the All-Nodes multicast address and to the Solicited-Node multicast addresses. This specification allows for two methods of supporting this multicast forwarding.

6.1.1 GMAC Explicit DSID Forwarding

This specification allows a DOCSIS 2.0+IPv6 CM to support GMAC Explicit DSID Forwarding as described in the GMAC-Explicit Multicast DSID Forwarding Mode section of [MULPIv3.0]. GMAC Explicit DSID Forwarding means that the DOCSIS 2.0+IPv6 CM supports DSID forwarding of multicast traffic per the DSID based Filtering and Forwarding by a Cable Modem section of [MULPIv3.0], but performs filtering of multicast traffic based on the Group MAC Address.

Prior to registration, a DOCSIS 2.0+IPv6 CM that is capable of GMAC Explicit DSID Forwarding MUST filter multicast traffic not addressed to the IPv6 Link Local Scope All Nodes Address or the Solicited Node Addresses. A DOCSIS 2.0+IPv6 CM that is capable of GMAC Explicit DSID Forwarding MUST learn the pre-registration DSID from the MDD message. The DOCSIS 2.0+IPv6 CM MUST forward pre-registration multicast traffic to its IP stack based on the pre-registration DSID as defined in the DSID based Filtering and Forwarding by a Cable Modem section of [MULPIv3.0].

A DOCSIS 2.0+IPv6 CM that is capable of GMAC Explicit DSID Forwarding MUST report the following capabilities in the Registration Request message:

- Multicast DSID Support (TLV 5.32) = number of multicast DSIDs supported by CM
- Multicast DSID Forwarding (TLV5.33) = 1
- Frame Control Type Forwarding (TLV 5.34) = 0 or 1

The CMTS may disable Multicast DSID Forwarding on the CM by confirming a value of 0 in the Multicast DSID Forwarding capability in the Registration Response message per [MULPIv3.0]. If the CMTS disables Multicast DSID Forwarding, the CM that is capable of GMAC Explicit DSID Forwarding MUST continue to forward to its IP stack packets addressed to the IPv6 All Nodes address, the Solicited Node multicast address calculated from its link-local address, and the Solicited Node multicast address calculated from the MSO assigned global IPv6 address. The CM performs IGMPv2 snooping per [RFIv2.0] and cannot forward IPv6 multicast to the CPE interfaces.

If the CMTS confirms a value of 1 in the Multicast DSID Forwarding capability in the Registration Response message, the CM that is capable of GMAC Explicit DSID Forwarding MUST stop forwarding multicast traffic labeled with the Pre-Registration DSID upon the receipt of the REG-RSP message. The CM MUST then begin forwarding Multicast traffic based on the DSIDs and Group MAC Addresses communicated in the Registration Response message. The CMTS includes multicast traffic addressed to the IPv6 Link Local Scope All Nodes

Address, and the CM's Solicited Node Addresses in the DSIDs and Group MAC Addresses communicated in the Registration Response message.

The GMAC Explicit CM MUST support the use of Multicast DSID Encodings (TLV 50.4) described in the Multicast Encodings section of [MULPIv3.0], as well as the Security Association Encodings (TLV 51) described in the Security Association Encoding section of [MULPIv3.0] in a Registration Response message.

The GMAC Explicit CM MUST support the use of the Dynamic Bonding Change mechanism per [MULPIv3.0] to maintain and learn new DSID values and Security Associations for IP Multicast. The GMAC Explicit CM performs a Dynamic Bonding Change (DBC) operation when it receives a DBC-REQ message containing only Multicast DSID Encodings (TLV 50.4), or Security Association Encodings (TLV 51). The DOCSIS 2.0+IPv6 CM MUST reject a DBC-REQ message with any encodings other than the Multicast DSID Encodings, or Security Association Encodings.

The GMAC Explicit CM MUST support DSID indexed PHS as described in Payload Header Suppression Header section of [MULPIv3.0].

6.1.2 IPv6 Multicast for MDF-incapable CMs

This specification alternatively allows a DOCSIS 2.0+IPv6 CM that is unable to implement DSID forwarding to support CPE IPv6 provisioning through other means. The MDF-incapable CM supports only the multicast forwarding necessary for provisioning of an IPv6 CPE.

Prior to registration, the MDF-incapable CM MUST forward packets addressed to the Well-Known IPv6 Addresses [MULPIv3.0], the Solicited Node multicast address calculated from its link-local address, and the Solicited Node multicast address calculated from the MSO assigned global IPv6 address to its IP stack. This CM requires no knowledge of the Pre-Registration DSID in order to forward this traffic.

The DOCSIS 2.0+IPv6 CM MUST signal support for multicast forwarding capabilities other than MDF by reporting the following capabilities in the Registration Request message:

- Multicast DSID Support (TLV 5.32) = 0
- Multicast DSID Forwarding (TLV5.33) = 0
- Frame Control Type Forwarding (TLV 5.34) = 0

After registration, the MDF-incapable CM MUST continue to forward to its IP stack packets addressed to the IPv6 All Nodes address, the Solicited Node multicast address calculated from its link-local address, and the Solicited Node multicast address calculated from the MSO assigned global IPv6 address.

The MDF-incapable CM MUST forward Neighbor Discovery packets sent to CPEs Solicited Node multicast IPv6 addresses and to the All-Nodes multicast address onto CPE ports, unless administratively prohibited via the configuration of filters.

The definition of the multicast forwarding mechanism for MDF-incapable CMs is vendor proprietary. The CM, for example, may forward onto CPE ports all traffic matching the multicast MAC address 33-33-FF-xx-xx-xx. As another example, the CM may learn CPE Solicited Node multicast addresses via snooping of the Neighbor Discovery, or Duplicate Address Detection packets sent by CPE, and forward traffic matching these addresses only.

6.2 Filtering IPv6 Traffic

In order to provide IPv6 filtering support for devices forwarding IPv6 traffic to the CMCI ports, the DOCSIS 2.0+IPv6 CM MAY support IPv6 classification and upstream drop classification per [MULPIv3.0]. If the DOCSIS

2.0+IPv6 CM supports IPv6 classification and upstream drop classification per [MULPIv3.0], it MUST report the number of Upstream Drop Classifiers it supports using the Upstream Drop Classification Support capability (TLV 5.38) in the Registration Request message.

For DOCSIS 2.0+IPv6 CMs that do not support Upstream Drop Classification, the MSO has the option of configuring the Subscriber Management MIB at the CMTS to perform this function. The DOCSIS 2.0+IPv6 CM MUST support the Subscriber Management CPE IPv6 Prefix List (TLV 61) and the Subscriber Management Control Max CPE IPv6 Prefix (TLV 63) as defined in [MULPIv3.0].

DOCSIS 2.0+IPv6 CMs MUST NOT transmit upstream IPv6 Router Advertisements (RAs) received on any interface.

7 MANAGEMENT

7.1 Simple Network Management Protocol (SNMP)

The DOCSIS 2.0+IPv6 CM MUST support SNMP over IPv6 as defined in the Requirements for IPv6 section in [OSSIv3.0].

7.2 MIB Module Updates

In order to accommodate the introduction of IPv6 addresses, several of the DOCSIS 2.0 MIBs have been updated. The following sections detail the MIB implementations for the DOCSIS 2.0+IPv6 CM.

7.2.1 IP-MIB [RFC 4293]

The [RFC 4293] MIB is required in a DOCSIS 2.0+IPv6 CM. This MIB replaces both RFC 2011 and RFC 2012. This IP-MIB [RFC 4293] MUST be implemented per the guidelines in [OSSIv3.0].

7.2.2 DOCS-CABLE-DEVICE-MIB [RFC 4639]

A DOCSIS 2.0+IPv6 CM MUST support the requirements for [RFC 4639] defined in [OSSIv3.0].

7.2.3 DOCS-IF-MIB [OSSIv3.0]

A DOCSIS 2.0+IPv6 CM MUST support the RFI MIB in Detailed MIB Requirements Annex [OSSIv3.0]. The object docsIfCmStatusValue is extended to align with the DOCSIS 3.0 CmRegState Textual Convention in DOCS-IF3-MIB.

```
docsIfCmStatusValue OBJECT-TYPE
        SYNTAX      INTEGER {
             other(1),
             notReady(2),
             notSynchronized(3),
             phySynchronized(4),
             usParametersAcquired(5),
             rangingInProgress(22),
             rangingComplete(6),
             eaeInProgress(14), -- Not Applicable
             dhcpv4InProgress(15),
             dhcpv6InProgress(16),
             dhcpv4Complete(7),
             dhcpv6Complete(17),
             todEstablished(8),
             securityEstablished(9),
             configFileDownloadComplete(10),
             registrationInProgress(18),
             registrationComplete(11),
             accessDenied(13),
             operational(12),
             bpiInit(19),
             forwardingDisabled(20),
             dsTopologyResolutionInProgress(21) -- Not Applicable
}

        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
```

```
            "Current Cable Modem connectivity state, as specified
             in the RF Interface Specification. Interpretations for
             state values. This list has been modified for DOCSIS 2.0
             CM supporting IPv6 to align it with the states identified
             In the CmRegState TC.
             The state value accessDenied(13) indicates the CMTS has
             sent a Registration Aborted message to the CM. The same
             state is reported as accessDenied(7) by the CMTS object
             docsIfCmtsCmStatusValue."
        REFERENCE
            "Data-Over-Cable Service Interface Specifications: Radio
             Frequency Interface Specification SP-RFIv2.0-CO2-090422,
             Section 11.2.
             Data-Over-Cable Service Interface Specifications:
             Operations Support System Interface Specification
             SP-OSSIv2.0-CO1-081104, Section 6.3.4.2.
             Data-Over-Cable Service Interface Specifications
             DOCSIS 3.0 Operations Support System Interface
             Specification: CM-SP-OSSIv3.0-I08-090121."
```

7.2.4 UDP-MIB [RFC 4113]

DOCSIS 2.0 defines the use of the UDP MIB [RFC 2013]. This version of the MIB module has since been updated in [RFC 4113]. The DOCSIS 2.0 CM that supports IPv6 MAY implement [RFC 4113] per [OSSIv3.0]. The DOCSIS 2.0 CM that supports IPv6 MAY implement [RFC 2013] per [OSSIv3.0].

7.2.5 IGMP-STD-MIB [RFC 2933]

DOCSIS 2.0 requires the implementation of the IGMP-STD-MIB [RFC 2933]. This MIB only supports IGMPv2 multicast groups. When GMAC Explicit Multicast DSID Forwarding is enabled, the use of the IGMP-STD-MIB [RFC 2933] is not required.

7.2.6 DOCS-QOS-MIB [OSSIv3.0] and DOCS-QOS3-MIB [OSSIv3.0]

A DOCSIS 2.0+IPv6 CM MUST support the DOCS-QOS-MIB [OSSIv3.0]. DOCSIS 2.0+IPv6 CMs that support Upstream Drop Classifiers (UDCs) and IPv6 packet classification MUST support the MIB object definitions for the docsQosPktClassTable from DOCS-QOS3-MIB [OSSIv3.0] rather than the definitions for docsQosPktClassTable in DOCS-QOS-MIB [OSSIv3.0].

A DOCSIS 2.0+IPv6 CM that supports GMAC Explicit Multicast DSID Forwarding MUST support the following CM DSID MIB objects from the DOCS-QOS3-MIB [OSSIv3.0].

```
docsQosCmDsidTable
    docsQosCmDsidEntry
        docsQosCmDsidDsid
        docsQosCmDsidUsage
        docsQosCmDsidCmInterfaceMask
        docsQosCmDsidFwdCmInterfaceMask
docsQosCmDsidClientTable
    docsQosCmDsidClientEntry
        docsQosCmDsidClientDsid
        docsQosCmDsidClientClientMacId
        docsQosCmDsidClientClientMacAddr
```

The DOCSIS 2.0+IPv6 CM that supports GMAC Explicit Multicast DSID Forwarding MAY implement the docsQosCmDsidStatsTable, and if supported, the following objects are included.

```
docsQosCmDsidStatsTable
    docsQosCmDsidStatsEntry
        docsQosCmDsidStatsDsid
        docsQosCmDsidStatsNumPackets
```

The omitted columnar objects from the CmDsid tables identified above should return a "noSuchObject" when read by a SNMP Manager.

7.2.7 DOCS-IF3-MIB [OSSIv3.0]

DOCSIS 2.0+IPv6 CMs that support IPv6 provisioning MUST support docsIf3CmMdCfgTable from the DOCS-IF3-MIB [OSSIv3.0].

7.3 DOCSIS Events

The DOCSIS 2.0+IPv6 CM MUST implement the events listed in the CM Configuration Interface Specification Annex in [OSSIv3.0]. Some of the Event Ids occur in both [OSSIv3.0] and [OSSIv3.0]. An Event ID from [OSSIv3.0] listed below supersedes the same Event ID from [OSSIv3.0].

The following DHCP Event Ids from [OSSIv3.0] MUST be used when the DOCSIS 2.0+IPv6 CM is operating with an IPv4 Management Stack:

- 68000100
- 68000200
- 68000300
- 68000301

The following Event Ids from [OSSIv3.0] MUST be supported by the DOCSIS 2.0+IPv6 CM for support of IPv6 Management Stack:

- 68001200
- 68001201
- 68001202
- 68001203
- 68001301
- 68001302
- 68010500

The following Event Ids from [OSSIv3.0] MUST be supported by the DOCSIS 2.0+IPv6 CM that supports the optional APM or Dual Stack provisioning modes:

- 68010700
- 68001204
- 68001205

The following Event Ids from [OSSIv3.0] MUST be supported by the DOCSIS 2.0+IPv6 CM for support of IPv6 and IPv4 lease renewal events:

- 68010100
- 68010200
- 68010300
- 68010400
- 68010600

The following Event Ids from [OSSIv3.0] MUST be supported by the DOCSIS 2.0+IPv6 CM for support of ToD operations over IPv4 or IPv6:

- 68000403
- 68000404

The following Event Ids from [OSSIv3.0] MUST be supported by the DOCSIS 2.0+IPv6 CM for support of IPv6 and IPv4 software upgrade events:

- 69010100
- 69010200
- 69010300
- 69010400
- 69010500
- 69010600
- 69010700
- 69010800
- 69010900
- 69011000
- 69011100
- 69011200
- 69020100
- 69020200
- 69020300
- 69020400
- 69020500
- 69020600
- 69020700
- 69020800
- 69020900

7.4 SNMP Access Requirements

Support for both NmAccess and SNMP Coexistence is required for a DOCSIS 2.0+IPv6 CM with some changes. The SNMP access method Open Access defined in DOCSIS 2.0 is deprecated for the DOCSIS 2.0+IPv6 CM. When defining SNMP Coexistence parameters, the DOCSIS 2.0+IPv6 CM MUST support the enhancements to the SNMP Target Address Table defined in [RFC 3419]. The DOCSIS 2.0+IPv6 CM also accepts the SNMP Access configuration file TLVs defined in [MULPIv3.0] and [OSSIv3.0], including the SNMPv3 Notification Receiver TLV. These encodings allow for the configuration of IPv6 address in the SNMP Coexistence and SNMPv3 frameworks.

It is also important to note that NmAccess configurations settings in the CM config file do not allow for IPv6 addresses. As a result, if a DOCSIS 2.0+IPv6 CM receives a configuration file with NmAccess settings and is provisioned in any IPv6 provisioning mode, the DOCSIS 2.0+IPv6 CM may be unmanageable. When the DOCSIS 2.0+IPv6 CM is provisioned for IPv6, the SNMP Access method needs to be configured with SNMP Coexistence or SNMPv3 enabled.

If the DOCSIS 2.0+IPv6 CM receives a configuration file that does not contain any SNMP configuration TLVs, the DOCSIS 2.0+IPv6 CM will become unmanageable via SNMP after registration [OSSIv3.0]. The use of CMTS tools (e.g., Ranging Abort) to reset a modem will be needed to force the modem to re-initialize and acquire a new configuration file.

Configuration of NmAccess and Coexistence modes are accomplished through the CM configuration file TLVs. DOCSIS 2.0 CMs support the use of configuration TLVs defined in [RFIv2.0]:

- SNMP Write-Access Control (TLV 10)
- SNMP MIB Object (TLV 11)
- SNMPv3 Kickstart Value (TLV 34)

In addition, the DOCSIS 2.0+IPv6 CM MUST support the following SNMP Configuration TLVs defined in [MULPIv3.0]:

- SNMPv3 Notification Receiver (TLV 38)
- SNMPv1v2c Coexistence Configuration (TLV 53)
- SNMPv3 Access View Configuration (TLV 54)
- SNMP CPE Access Control (TLV 55)

The configuration TLVs 53 and 54 allow the operator to configure community string and SNMP Coexistence tables in a highly efficient manner where TLV-11 has been used in DOCSIS 2.0. The DOCSIS 2.0+IPv6 CM MUST support the definition of TLV38 from MULPI in order to support the needed IPv6 transport and trap receiver encodings when the DOCSIS 2.0+IPv6 CM is provisioned with an IPv6 single or Dual Stack configuration. TLV 55 also provides an optimization to enable or disable SNMP Access from the CMCI ports.

8 CABLE MODEM SOFTWARE DOWNLOAD

The DOCSIS 2.0+IPv6 CM allows both SNMP-initiated and configuration-file-initiated software downloads over IPv6. The DOCSIS 2.0+IPv6 CM MUST implement the docsDevSoftware group [RFC 4639] for the management and initiation of upgrades. The DOCSIS 2.0+IPv6 CM MUST support the Software Upgrade IPv6 TFTP Server TLV (TLV 58) defined in [MULPIv3.0] for downloads triggered via the configuration file. For these downloads, the DOCSIS 2.0+IPv6 CM MUST select the software server as defined in the Downloading Cable Modem Operating Software section of [MULPIv3.0].

If the DOCSIS 2.0+IPv6 CM receives an ICMP Destination Unreachable message or ICMP port unreachable message for the TFTP server at any time during the firmware download process, the DOCSIS 2.0+IPv6 CM MUST terminate the firmware download on the TFTP server whose address is included in the ICMP Destination Unreachable message without performing the TFTP Request Retries nor the TFTP Download Retries [RFIv2.0].

Appendix I DHCPv6 Options (Informative)

The table below shows all of the DOCSIS defined DHCPv6 options used by a DOCSIS 2.0+IPv6 CM during IPv6 provisioning. Some of these options are specific to certain types of embedded implementations and are not required for all devices.

Table 1 – DHCPv6 Options

Option Number	Option Name	Reference
1	Client Identifier option (DUID)	[RFC 3315]
2	Server Identifier Option	[RFC 3315]
3	IA_NA option (Ipv6 address)	[RFC 3315]
6	Option Request Option	[RFC 3315]
14	Rapid Commit Option	[RFC 3315]
16	Vendor Class	[RFC 3315]
19	Reconfigure Message option	[RFC 3315]
20	Reconfigure Accept Option	[RFC 3315]
17	Vendor-specific information option	

Option Number	Option Name	Reference
1	CL Option Request option	[CANN-DHCP-Reg]
32	TFTP Server Addresses option	[CANN-DHCP-Reg]
33	Configuration File Name option	[CANN-DHCP-Reg]
34	Syslog Server Addresses option	[CANN-DHCP-Reg]
35	TLV5 Encoding	[CANN-DHCP-Reg]
36	DOCSIS Device Identifier option	[CANN-DHCP-Reg]
0x087A	CableLabs client configuration (Applicable only for eDOCSIS devices with eCM+eMTA)	[CANN-DHCP-Reg]
37	Time Protocol Servers option	[CANN-DHCP-Reg]
38	Time Offset option	[CANN-DHCP-Reg]