



***Society of Cable
Telecommunications
Engineers***

**ENGINEERING COMMITTEE
Data Standards Subcommittee**

AMERICAN NATIONAL STANDARD

ANSI/SCTE 79-2 2009

DOCSIS 2.0 Part 2: Operations Support System Interface

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability 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, whether used domestically or internationally.

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

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, 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 standard 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>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2009
140 Philips Road
Exton, PA 19341

Note: DOCSIS® is a registered trademark of Cable Television Laboratories, Inc., and is used in this document with permission.

Table of Contents

1	SCOPE AND PURPOSE	1
1.1	SCOPE	1
1.2	REQUIREMENTS	1
2	REFERENCES (NORMATIVE/INFORMATIVE)	2
3	GLOSSARY (INFORMATIVE)	5
4	ABBREVIATIONS	16
5	SNMP PROTOCOL	19
5.1	SNMP MODE FOR DOCSIS 2.0-COMPLIANT CMTSES	19
5.1.1	Key Change Mechanism	20
5.2	SNMP MODE FOR DOCSIS 2.0-COMPLIANT CMS	20
5.2.1	SNMPv3 Initialization and Key changes	22
5.2.2	SNMPv3 Initialization	22
5.2.3	DH Key Changes	24
5.2.4	VACM Profile	24
6	MANAGEMENT INFORMATION BASES (MIBS)	27
6.1	IPCDN DRAFTS AND OTHERS	27
6.2	IETF RFCs	28
6.3	MANAGED OBJECTS REQUIREMENTS	28
6.3.1	CMTS MIB requirements	28
6.3.2	Requirements for [RFC 2669]	28
6.3.3	Requirements for DOCS-IF-MIB	28
6.3.4	Requirements for [RFC 2863]	30
6.3.5	Interface MIB and Trap Enable	33
6.3.6	Requirements for [RFC 2665]	33
6.3.7	Requirements for [RFC 1493]	33
6.3.8	Requirements for [RFC 2011]	33
6.3.9	Requirements for [RFC 2013]	34
6.3.10	Requirements for [RFC 3418]	34
6.3.11	Requirements for DOCS-QOS-MIB	34
6.3.12	Requirements for "draft-ietf-ipcdn-igmp-mib-01.txt"	34
6.3.13	Requirements for [RFC 2933]	34
6.3.14	Requirements for DOCS-BPI2-MIB	34
6.3.15	Requirements for USB MIB	34
6.3.16	Requirements for DOCS-SUBMGT-MIB	35
6.3.17	Requirements for [RFC 2786]	35
6.3.18	Requirements for [RFC 3083]	35
6.3.19	Requirements for DOCS-IF-EXT-MIB	35
6.3.20	Requirements for DOCS-CABLE-DEVICE-TRAP-MIB	35
6.3.21	Requirements for SNMPv3 MIBs	36
6.3.22	Requirements for DOCS-LOADBALANCING-MIB	36
6.3.23	Requirements for DOCS-IFEXT2-MIB	36
6.4	CM CONFIGURATION FILES, TLV-11 AND MIB OIDS/VALUES	36
6.4.1	CM configuration file TLV-11 element translation (to SNMP PDU)	36
6.4.2	CM configuration TLV-11 elements not supported by the CM	37
6.4.3	CM state after CM configuration file processing success	37
6.4.4	CM state after CM configuration file processing failure	37
6.5	TREATMENT AND INTERPRETATION OF MIB COUNTERS ON THE CM	37

6.6	SNMPV3 NOTIFICATION RECEIVER CONFIG FILE ELEMENT	38
6.6.1	Mapping of TLV fields into created SNMPv3 table rows.....	38
7	OSSI FOR RADIO FREQUENCY INTERFACE	45
7.1	SUBSCRIBER ACCOUNT MANAGEMENT INTERFACE SPECIFICATION	45
7.1.1	Subscriber Usage Billing and class of services	45
7.1.2	IP Detail Record (IPDR) Standard.....	51
7.1.3	DOCSIS Subscriber Usage Billing Requirements.....	63
7.2	CONFIGURATION MANAGEMENT	73
7.2.1	Version Control	74
7.2.2	System Initialization and Configuration	75
7.2.3	Secure Software Upgrades.....	75
7.3	PROTOCOL FILTERS	79
7.3.1	LLC filters.....	80
7.3.2	Special filters	80
7.3.3	IP spoofing filter	80
7.3.4	SNMP Access Filter	81
7.3.5	IP filter.....	81
7.4	FAULT MANAGEMENT	82
7.4.1	SNMP Usage.....	82
7.4.2	Event Notification	85
7.4.3	Throttling, Limiting and Priority for Event, Trap and Syslog	92
7.4.4	Non-SNMP Fault Management Protocols	93
7.5	PERFORMANCE MANAGEMENT	93
7.5.1	Additional MIB implementation requirements.....	94
7.6	COEXISTENCE	94
7.6.1	Coexistence and MIBs	95
7.6.2	Coexistence and SNMP.....	97
8	OSSI FOR BPI+	98
8.1	DOCSIS ROOT CA.....	98
8.2	DIGITAL CERTIFICATE VALIDITY PERIOD AND RE-ISSUANCE	98
8.2.1	DOCSIS Root CA Certificate.....	98
8.2.2	DOCSIS Manufacturer CA Certificate	98
8.2.3	DOCSIS CM Certificate.....	99
8.2.4	DOCSIS Code Verification Certificate	99
8.3	CM CODE FILE SIGNING POLICY	99
8.3.1	Manufacturer CM Code File Signing Policy	99
9	OSSI FOR CMCI.....	101
9.1	SNMP ACCESS VIA CMCI.....	101
9.2	CONSOLE ACCESS.....	101
9.3	CM DIAGNOSTIC CAPABILITIES	102
9.4	PROTOCOL FILTERING	102
9.5	MANAGEMENT INFORMATION BASE (MIB) REQUIREMENTS	102
10	CM OPERATIONAL STATUS VISUALIZATION	103
10.1	CM LEDS REQUIREMENTS AND OPERATION	103
10.1.1	Power and self test.....	103
10.1.2	Scanning and Synchronization to Downstream	104
10.1.3	DOCSIS Upstream obtaining parameters.....	104
10.1.4	Becoming Operational.....	104
10.1.5	Data Link and Activity	104
10.2	ADDITIONAL CM OPERATIONAL STATUS VISUALIZATION FEATURES	104
10.2.1	Software Download	104

ANNEX A	DETAILED MIB REQUIREMENTS (NORMATIVE)	105
A.1	IF-MIB IFTable MIB-Object Details	139
A.2	[RFC 1493] AND [RFC 2863] MIB-Object Details FOR CCCM	153
A.2.1	[RFC 1493] MIB-Object Details	153
A.2.2	Implementation of [RFC 1493] MIB for CCCM	154
A.2.3	[RFC 2863] ifTable MIB-Object details for CCCM	156
ANNEX B	IPDR STANDARDS SUBMISSION FOR DOCSIS CABLE DATA SYSTEMS SUBSCRIBER USAGE BILLING RECORDS	157
B.1	SERVICE DEFINITION	157
B.1.1	DOCSIS Service Requirements	157
B.1.2	DOCSIS IPDR Service Usage Element List	158
B.2	DOCSIS IPDR SUBSCRIBER USAGE BILLING SERVICE SCHEMA	163
B.2.1	DOCSIS IPDR Schema File DOCSIS-3.5.1-A.0.xsd	163
ANNEX C	SNMPV2C INFORM REQUEST DEFINITION FOR SUBSCRIBER ACCOUNT MANAGEMENT (SAM) (NORMATIVE)	169
ANNEX D	FORMAT AND CONTENT FOR EVENT, SYSLOG, AND SNMP TRAP (NORMATIVE)	170
ANNEX E	APPLICATION OF [RFC 2933] TO DOCSIS 2.0 ACTIVE/PASSIVE IGMP DEVICES (NORMATIVE)	195
E.1	DOCSIS 2.0 IGMP MIBs	195
E.1.1	IGMP Capabilities: Active and Passive Mode	195
E.1.2	IGMP Interfaces	195
E.2	DOCSIS 2.0 CM SUPPORT FOR THE IGMP MIB	195
E.2.1	igmpInterfaceTable- igmpInterfaceEntry	195
E.2.2	igmpCacheTable - igmpCacheEntry	199
E.3	DOCSIS 2.0 CMTS SUPPORT FOR THE IGMP MIB	201
E.3.1	igmpInterfaceTable- igmpInterfaceEntry	201
E.3.2	igmpCacheTable - igmpCacheEntry	205
E.3.3	IGMP MIB Compliance	207
E.3.4	MIB Groups	208
ANNEX F	EXPECTED BEHAVIORS FOR DOCSIS 2.0 MODEM IN 1.0, 1.1, AND 2.0 MODES IN OSS AREA (NORMATIVE)	210
ANNEX G	DOCS-IF-EXT-MIB (NORMATIVE)	212
ANNEX H	DOCS-CABLE-DEVICE-TRAP-MIB (NORMATIVE)	215
ANNEX I	REQUIREMENTS FOR DOCS-LOADBALANCING-MIB (MANDATORY)	229
ANNEX J	REQUIREMENTS FOR DOCS-QOS-MIB (MANDATORY)	248
ANNEX K	REQUIREMENTS FOR DOCS-IFEXT2-MIB (MANDATORY)	292
ANNEX L	DOCS-SUBMGT-MIB (MANDATORY)	302
APPENDIX I	BUSINESS PROCESS SCENARIOS FOR SUBSCRIBER ACCOUNT MANAGEMENT (INFORMATIVE)	318
I.1	THE OLD SERVICE MODEL: "ONE CLASS ONLY" AND "BEST-EFFORT" SERVICE	318
I.2	THE OLD BILLING MODEL: "FLAT RATE" ACCESS	318
I.3	A SUCCESSFUL NEW BUSINESS PARADIGM	318
I.3.1	Integrating "front end" processes seamlessly with "back office" functions	319

I.3.2	<i>Designing Classes of Services</i>	319
I.3.3	<i>Usage-Based Billing</i>	320
I.3.4	<i>Designing Usage-Based Billing Models</i>	320
APPENDIX II SUMMARY OF CM AUTHENTICATION AND CODE FILE AUTHENTICATION (INFORMATIVE)321		
II.1	AUTHENTICATION OF THE DOCSIS 2.0-COMPLIANT CM	321
II.1.1	<i>Responsibility of the DOCSIS Root CA</i>	321
II.1.2	<i>Responsibility of the CM manufacturers</i>	322
II.1.3	<i>Responsibility of the operators</i>	322
II.2	AUTHENTICATION OF THE CODE FILE FOR THE DOCSIS 2.0-COMPLIANT CM	322
II.2.1	<i>Responsibility of the DOCSIS Root CA</i>	323
II.2.2	<i>Responsibility of the CM manufacturer</i>	323
II.2.3	<i>Responsibility of CableLabs</i>	324
II.2.4	<i>Responsibility of the operators</i>	324
APPENDIX III ENCODING EXAMPLES FOR SUBSCRIBER USAGE IPDRS 325		
III.1	EXAMPLE USAGE RECORD STREAMING MODEL CONTAINING DIVERSE SERVICES	325

List of Figures

FIGURE 6-1 - IFINDEX EXAMPLE FOR CMTS	31
FIGURE 6-2 - IFINDEX EXAMPLE FOR CM.....	31
FIGURE 7-1 - SUBSCRIBER USAGE BILLING MODEL MAPPING TO DOCSIS MANAGEMENT OBJECTS.....	50
FIGURE 7-2 - BASIC NETWORK MODEL (REF. [IPDR/BSR] FROM WWW.IPDR.ORG)	52
FIGURE 7-3 - IPDRDOC 3.5 GENERIC SCHEMA.....	53
FIGURE 7-4 - DOCSIS IPDR 3.5 XML SCHEMA FOR DOCSIS SERVICE SPECIFICATION	54
FIGURE 7-5 - BILLING COLLECTION INTERVAL EXAMPLE.....	60
FIGURE 7-6 - IPDR/SP SIMPLE STATE DIAGRAM	65
FIGURE 7-7 - FLOW DIAGRAM FOR DOCSIS DEFAULT STREAMING REQUIREMENTS	66
FIGURE 7-8 - MANUFACTURER CONTROL SCHEME.....	75
FIGURE 7-9 - OPERATOR CONTROL SCHEME	76
FIGURE 7-10 - COEXISTENCE (DOCSIS 1.0 MODE VS. DOCSIS 1.1 MODE VS. DOCSIS 2.0 MODE)	94
FIGURE II-1 - AUTHENTICATION OF THE DOCSIS 2.0-COMPLIANT CM.....	321
FIGURE II-2 - AUTHENTICATION OF THE CODE FILE FOR THE DOCSIS 2.0-COMPLIANT CM.....	323
FIGURE III-1 - SET OF CM SERVICES IN AN ARBITRARY PERIOD OF TIME (LEFT GRAPHIC) SET OF RECORDS ASSOCIATED TO THE COLLECTION INTERVAL 10:30 TO 11:00 AM (RIGHT GRAPHIC)	326

List of Tables

TABLE 6-1 - IPCDN DRAFTS	27
TABLE 6-2 - IETF RFCs	28
TABLE 6-3 - CM INTERFACE NUMBERING	32
TABLE 6-4 - DOCSIfCMSTATUSVALUE AND IFOPERSTATUS RELATIONSHIP	32
TABLE 6-5 - SNMPNOTIFYTABLE	39
TABLE 6-6 - SNMPTARGETADDRTABLE	39
TABLE 6-7 - SNMPTARGETADDREXTTABLE	40
TABLE 6-8 - SNMPTARGETPARAMSTABLE FOR <TRAP TYPE> 1, 2, OR 3	40
TABLE 6-9 - SNMPTARGETPARAMSTABLE FOR <TRAP TYPE> 4 OR 5	40
TABLE 6-10 - SNMPNOTIFYFILTERPROFILETABLE	41
TABLE 6-11 - SNMPNOTIFYFILTERTABLE	41
TABLE 6-12 - SNMPCOMMUNITYTABLE	42
TABLE 6-13 - USMUSERTABLE	42
TABLE 6-14 - VACMSECURITYTOGROUPTABLE	43
TABLE 6-15 - VACMACCESSTABLE	43
TABLE 6-16 - VACMVIEWTREEFAMILYTABLE	44
TABLE 7-1 - DEFAULT DOCSIS STREAMING FLOW DIAGRAM	67
TABLE 7-2 - SAMPLE DOCSDEVNMACCESSIP VALUES	81
TABLE 7-3 - DEFAULT EVENT PRIORITIES FOR THE CABLE MODEM DEVICE	90
TABLE 7-4 - DEFAULT EVENT PRIORITIES FOR THE CMTS SUPPORTING ONLY LOCAL-LOG NON-VOLATILE	91
TABLE 7-5 - DEFAULT EVENT PRIORITIES FOR THE CMTS SUPPORTING ONLY LOCAL-LOG VOLATILE	91
TABLE 7-6 - DEFAULT EVENT PRIORITIES FOR THE CMTS SUPPORTING BOTH LOCAL-LOG NON-VOLATILE AND LOCAL-LOG VOLATILE	91
TABLE 7-7 - EVENT PRIORITIES ASSIGNMENT FOR CMS AND CMTSES	92
TABLE 7-8 - MAXIMUM LEVEL OF SUPPORT FOR CM EVENTS	92
TABLE 7-9 - MAXIMUM LEVEL OF SUPPORT FOR CMTS EVENTS	93
TABLE 7-10 - DOCSIS 2.0 CM MODES AND MIB REQUIREMENTS	95
TABLE A-1 - [RFC 1493] MIB-OBJECT DETAILS	153
TABLE A-2 - THE DOT1DBASE GROUP	154
TABLE A-3 - DOT1DBASEPORTTABLE	155
TABLE A-4 - DOT1DBASEPORTTABLE	155
TABLE A-5 - DOT1DFDBTABLE	155
TABLE A-6 - DOT1DTpPORTTABLE	155
TABLE A-7 - [RFC 2863] IFTABLE MIB-OBJECT DETAILS FOR CCCM	156
TABLE B-1 - SERVICE USAGE ELEMENT NAMES	162
TABLE III-1 - SAMPLE OF RECORDS FOR THE PERIOD 10:30 TO 11:00 AM	325

This page left blank intentionally.

1 SCOPE AND PURPOSE

1.1 Scope

This specification defines the Network Management requirements to support a DOCSIS 2.0 environment. More specifically, the specification details the SNMPv3 protocol and how it coexists with SNMP v1/v2. The RFCs and Management Information Base (MIB) requirements are detailed as well as interface numbering, filtering, event notifications, etc. Basic network-management principles such as account, configuration, fault, and performance management are incorporated in this specification for better understanding of managing a high-speed cable modem environment.

1.2 Requirements

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

“MUST”	This word or the adjective “REQUIRED” 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 or the adjective “RECOMMENDED” 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 or the adjective “OPTIONAL” 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.

This document defines many features and parameters, and a valid range for each parameter is usually specified. Equipment (CM and CMTS) requirements are always explicitly stated. Equipment must comply with all mandatory (MUST and MUST NOT) requirements to be considered compliant with this specification. Support of non-mandatory features and parameter values is optional.

2 REFERENCES (NORMATIVE/INFORMATIVE)

The following documents contain provisions, which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

- [DOCSIS 1] DOCSIS Cable Modem Termination System - Network-Side Interface Specification, CM-SP-CMTS-NSI-I01-960702, July 2, 1996, Cable Television Laboratories, Inc.
- [DOCSIS 2] DOCSIS Cable Modem to Customer Premise Equipment Interface Specification, CM-SP-CMCI-C01-081104, November 04, 2008, Cable Television Laboratories, Inc.
- [DOCSIS 4] DOCSIS Cable Modem Telephony Return Interface Specification, CM-SP-CMTRI-I01-970804, August 4, 1997, Cable Television Laboratories, Inc.
- [ID-IGMP] Fenner, W., IGMP-based Multicast Forwarding ("IGMP Proxying"), IETF Internet Draft, <http://www.ietf.org/internet-drafts/draft-fenner-igmp-proxy-03.txt>.
- [IETF3] draft-ietf-ipcdn-igmp-mib-00.txt, H. Abramson, "DOCSIS 1.1 IGMP MIB," June 1999.
- [IETF6] Proposed Standard RFC version of BPI+ MIB, "draft-ietf-ipcdn-bpiplus-05.txt."
- [IETF7] IETF Proposed Standard RFC-version of USB MIB.
- [IETF9] Proposed Standard RFC version of Customer Management MIB, "draft-ietf-ipcdn-subscriber-mib-02.txt."
- [IETF10] S. Cheshire, B. Aboba, and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses," internet-draft draft-ietf-zeroconf-ipv4-linklocal-10.txt.
- [IETF11] Raftus David, Goren Aviv, "Proposed Standard RFC version of Radio Frequency (RF) Interface Mib," draft-ietf-ipcdn-docs-rfmibv2-05.txt.
- [IPDR/BSR] "IPDR Business Solution Requirements" - Network Data Management Usage (NDM-U), Version 3.5.0.1, IPDR.org, May 2004.
- [IPDR/SSDG] "IPDR Service Specification Design Guide," Version 3.5.1, IPDR.org, November 2004.
- [IPDR/SP] "IPDR/Streaming Protocol Specification," Version 2.1, IPDR.org, November 2004.
- [IPDR/XDR] "IPDR/XDR File Encoding Format," Version 3.5.1, November 2004.
- [IPDR/CAPAB] "IPDR/Capability File Format," Version 3.5.0.1, IPDR.org, January 2004.
- [IPDR/XML] "IPDR/XML File Encoding Format," Version 3.5.0.1, IPDR.org, April 2004.
- [IPDR/FILE] "IPDR/File Transfer Protocol," Version 3.5.0.1, IPDR.org, April 2004.
- [ISO/IEC10038] ISO/IEC 10038 (ANSI/IEEE Std 802.1D): 1993, Information technology - Telecommunications and information exchange between systems - Local area networks - Media access control (MAC) bridges.
- [RFC 1157] Schoffstall, M., Fedor, M., Davin, J. and Case, J., A Simple Network Management Protocol (SNMP), May 1990.
- [RFC 1213] K. McCloghrie and M. Rose, Management Information Base for Network Management of TCP/IP-base internets: MIB-II, IETF, March 1991.
- [RFC 1224] L. Steinberg, Techniques for Managing Asynchronously Generated Alerts, May 1991.
- [RFC 1493] E. Decker, P. Langille, A. Rijssinghani, and K. McCloghrie, Definitions of Managed Objects for Bridges, July 1993.
- [RFC 1901] Case, J., McCloghrie, K., Rose, M. and S. Waldbusser, "Introduction to Community-based SNMPv2," January 1996.

- [RFC 1952] Deutsch, P., "GZIP file format specification version 4.3," May 1996.
- [RFC 2011] K. McCloghrie, "Category: Standards Track SNMPv2 Management Information Base for the Internet Protocol using SMIPv2," November 1996.
- [RFC 2013] K. McCloghrie, "Category: Standards Track SNMPv2 Management Information Base for the User Datagram Protocol using SMIPv2," November 1996.
- [RFC 2132] S. Alexander, R. Droms. DHCP Options and BOOTP Vendor Extensions, March 1997.
- [RFC 2246] Dierks, T. and C. Allen, "The TLS Protocol, Version 1.0," January 1999.
- [RFC 2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol," Nov 1998.
- [RFC 2576] R. Frye, D. Levi, S. Routhier, B. Wijnen, "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard and Network Management Framework," March 2000.
- [RFC 2578] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Structure of Management Information Version 2 (SMIPv2)," STD 58, April 1999.
- [RFC 2579] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Textual Conventions for SMIPv2," STD 58, April 1999.
- [RFC 2580] McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M. and S. Waldbusser, "Conformance Statements for SMIPv2," STD 58, April 1999.
- [RFC 2665] J. Flick, J. Johnson, "Definitions of Managed Objects for the Ethernet-like Interface Types," August 1999.
- [RFC 2669] M. St. Johns, "DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems," August 1999.
- [RFC 2670] M. St. Johns, "Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces," August 1999.
- [RFC 2786] stjohns-snmpv3-dhkeychange-mib-01.txt, Michael C. St. Johns, "Diffie-Helman USM Key MIB August 1999 Diffie-Helman USM Key Management Information Base and Textual Convention," Aug. 6, 1999.
- [RFC 2863] K. McCloghrie, F. Kastenholz, "The Interfaces Group MIB," June 2000.
- [RFC 2933] McCloghrie, K., Farinacci, D., Thaler, D., "Internet Group Management Protocol MIB," January 2007.
- [RFC 3083] R. Woundy, "Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems," RFC 3083, March 2001.
- [RFC 3410] J. Case, R. Mundy, D. Partain, B. Stewart, Introduction and Applicability Statements for Internet-Standard Management Framework, December 2002.
- [RFC 3411] D. Harrington, R. Presuhn, B. Wijnen, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, December 2002.
- [RFC 3412] J. Case, D. Harrington, R. Presuhn, B. Wijnen, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), December 2002.
- [RFC 3413] D. Levi, P. Meyer, B. Stewart, Simple Network Management Protocol (SNMP) Applications, December 2002.
- [RFC 3414] U. Blumenthal, B. Wijnen, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.
- [RFC 3415] B. Wijnen, R. Presuhn, K. McCloghrie, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002.
- [RFC 3416] R. Presuhn, Ed., Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), December 2002.

- [RFC 3417] R. Presuhn, Ed., Transport Mappings for the Simple Network Management Protocol (SNMP), December 2002.
- [RFC 3418] R. Presuhn, Ed., Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), December 2002.
- [RFC 3423] Zhang K, and E. Elkin, "XACCT's Common Reliable Accounting for Network Element (CRANE), Protocol Specification Version 1.0," RFC 3423, November 2002.
- [SCTE 23-2] ANSI/SCTE 23-2 2007, DOCSIS 1.1 Part 2: Baseline Privacy Plus Interface Specification.
- [SCTE 79-1] ANSI/SCTE 79-1 2009, DOCSIS 2.0 Part 1: Radio Frequency Interface.
- [SCTE 159-1] ANSI/SCTE 159-1 2008, IPCablecom Multimedia.
- [SCTE 165-4] SCTE 165-4 2009, IPCablecom 1.5 Part 4: Dynamic Quality-of-Service.
- [SMS] The Spectrum Management Application (SMA) and the Common Spectrum Management Interface (csmi), Time Warner Cable, December 24, 1995.
- [SYSLOG] R. C. Lonvick, "The BSD syslog Protocol," Informational RFC 3164, August 2001.

3 GLOSSARY (INFORMATIVE)

Active Service Flow

An admitted Service Flow from the CM to the CMTS which is available for packet transmission.

Address Resolution Protocol (ARP)

A protocol of the IETF for converting network addresses to 48-bit Ethernet addresses.

Admitted Service Flow

A Service Flow, either provisioned or dynamically signaled, which is authorized and for which resources have been reserved but is not active.

Allocation

A group of contiguous mini-slots in a MAP which constitute a single transmit opportunity.

American National Standards Institute (ANSI)

A US standards body.

Asynchronous Transfer Mode (ATM)

A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.

A-TDMA

DOCSIS 2.0 TDMA mode (as distinguished from DOCSIS 1.x TDMA).

Authorization Module

The authorization module is an abstract module that the CMTS can contact to authorize Service Flows and Classifiers. The authorization module tells the CMTS whether the requesting CM is authorized for the resources it is requesting.

Availability

In cable television systems, availability is the long-term ratio of the actual RF channel operation time to scheduled RF channel operation time (expressed as a percent value) and is based on a bit error rate (BER) assumption.

Bandwidth Allocation Map

The MAC Management Message that the CMTS uses to allocate transmission opportunities to CMs.

Bridge Protocol Data Unit (BDU)

Spanning tree protocol messages as defined in [ISO/IEC10038].

Broadcast Addresses

A predefined destination address that denotes the set of all data network service access points.

Burst

A single continuous RF signal from the upstream transmitter, from transmitter on to transmitter off.

Burst Error Second

Any Errored Second containing at least 100 errors.

Cable Modem (CM)

A modulator-demodulator at subscriber locations intended for use in conveying data communications on a cable.

Cable Modem Termination System (CMTS)

Cable modem termination system, located at the cable television system head-end or distribution hub, which provides complementary functionality to the cable modems to enable data connectivity to a wide-area network.

Cable Modem Termination System - Network Side Interface (CMTS-NSI)

The interface, defined in [DOCSIS 1], between a CMTS and the equipment on its network side.

Cable Modem to CPE Interface (CMCI)

The interface, defined in [DOCSIS 4], between a CM and CPE.

Carrier Hum Modulation

The peak-to-peak magnitude of the amplitude distortion relative to the RF carrier signal level due to the fundamental and low-order harmonics of the power-supply frequency.

Carrier-to-Noise Ratio (C/N or CNR)

The ratio of signal power to noise power in the defined measurement bandwidth. For digital modulation, $CNR = E_s/N_0$, the energy-per-symbol to noise-density ratio; the signal power is measured in the occupied bandwidth, and the noise power is normalized to the modulation-rate bandwidth. For video, the measurement bandwidth is 4 MHz.

CCCM

CPE Controlled Cable Modem. Refer to the DOCSIS Cable Modem to Customer Premise Equipment Interface (CMCI) specification.

Channel

The frequency spectrum occupied by a signal. Usually specified by center frequency and bandwidth parameters.

Chip

Each of the 128 bits comprising the S-CDMA spreading codes.

Chip Duration

The time to transmit one chip of the S-CDMA spreading code. The inverse of the chip rate.

Chip Rate

The rate at which individual chips of the S-CDMA spreading codes are transmitted. (1280 to 5120 kHz)

Classifier

A set of criteria used for packet matching according to TCP, UDP, IP, LLC, and/or 802.1P/Q packet fields. A classifier maps each packet to a Service Flow. A Downstream Classifier is used by the CMTS to assign packets to downstream service flows. An Upstream Classifier is used by the CM to assign packets to upstream service flows.

Code Hopping Matrix

A shifted version of the reference code matrix (see below) that is used when code hopping is employed to vary the codes used by each CM. The Code Hopping Matrix is either 128 rows by 128 columns (when all 128 codes are active) or is 127 rows by 128 columns (when less than 128 codes are active in the S-CDMA spreader-on frame). When less than 128 codes are active, Code 0 (all ones) is deleted from the matrix, but all remaining codes are still cycled through even if less than 127 codes are active in a frame.

Composite Second Order Beat (CSO)

The peak of the average level of distortion products due to second-order non-linearities in cable system equipment.

Composite Triple Beat (CTB)

The peak of the average level of distortion components due to third-order non-linearities in cable system equipment.

Cross-Modulation

A form of television signal distortion where modulation from one or more television channels is imposed on another channel or channels.

Customer

See End User.

Customer Premises Equipment (CPE)

Equipment at the end user's premises; MAY be provided by the end user or the service provider.

Data Link Layer

Layer 2 in the Open System Interconnection (OSI) architecture; the layer that provides services to transfer data over the transmission link between open systems.

Distribution Hub

A location in a cable television network which performs the functions of a head-end for customers in its immediate area, and which receives some or all of its television program material from a Master Head-end in the same metropolitan or regional area.

Downstream

In cable television, the direction of transmission from the head-end to the subscriber.

Drop Cable

Coaxial cable that connects to a residence or service location from a directional coupler (tap) on the nearest coaxial feeder cable.

Dynamic Host Configuration Protocol (DHCP)

An Internet protocol used for assigning network-layer (IP) addresses.

Dynamic Range

The ratio between the greatest signal power that can be transmitted over a multichannel analog transmission system without exceeding distortion or other performance limits, and the least signal power that can be utilized without exceeding noise, error rate or other performance limits.

Electronic Industries Association (EIA)

A voluntary body of manufacturers which, among other activities, prepares and publishes standards.

End User

A human being, organization, or telecommunications system that accesses the network in order to communicate via the services provided by the network.

Engineering Change Notice

The final step in the procedure to change specifications.

Engineering Change Order

The second step in the procedure to change specifications. DOCSIS posts ECO to web site EC table and ECO page (with indication of ECO Comment Deadline). DOCSIS issues ECO announcement to DOCSIS-announce and working group mail lists (with indication of ECO Comment Deadline).

Engineering Change Request

The first step in the procedure to change specifications. DOCSIS issues ECR number, posts to web site EC table and ECR page. DOCSIS sends ECR to subject area working group mail list (and author).

Errored Second

Any 1-sec interval containing at least one bit error.

Extended Subsplit

A frequency division scheme that allows bidirectional traffic on a single coaxial cable. Reverse path signals come to the head-end from 5 to 42 MHz. Forward path signals go from the head-end from 50 or 54 MHz to the upper frequency limit.

Feeder Cable

Coaxial cables that run along streets within the served area and connect between the individual taps which serve the customer drops.

Fiber Distributed Data Interface (FDDI)

A fiber-based LAN standard.

Fiber Node

A point of interface between a fiber trunk and the coaxial distribution.

Forward Channel

The direction of RF signal flow away from the head-end toward the end user; equivalent to Downstream.

Frame

See MAC frame, S-CDMA frame, and MPEG frame.

Group Delay

The difference in transmission time between the highest and lowest of several frequencies through a device, circuit or system.

Guard Time

Minimum time allocated between bursts in the upstream referenced from the symbol center of the last symbol of a burst to the symbol center of the first symbol of the following burst. The guard time should be at least the duration of five symbols plus the maximum system timing error.

Harmonic Related Carrier (HRC)

A method of spacing television channels on a cable television system in exact 6-MHz increments, with all carrier frequencies harmonically related to a common reference.

Head-end

The central location on the cable network that is responsible for injecting broadcast video and other signals in the downstream direction. See also Master Head-End, Distribution Hub.

Header

Protocol control information located at the beginning of a protocol data unit.

High Frequency (HF)

Used in this document to refer to the entire subsplit (5-30 MHz) and extended subsplit (5-42 MHz) band used in reverse channel communications over the cable television network.

High Return

A frequency division scheme that allows bi-directional traffic on a single coaxial cable. Reverse channel signals propagate to the head-end above the downstream passband.

Hum Modulation

Undesired modulation of the television visual carrier by the fundamental or low-order harmonics of the power supply frequency, or other low-frequency disturbances.

Hybrid Fiber/Coax (HFC) System

A broadband bidirectional shared-media transmission system using fiber trunks between the head-end and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.

Incremental Related Carriers (IRC)

A method of spacing NTSC television channels on a cable television system in which all channels except 5 and 6 correspond to the standard channel plan, used to reduce composite triple beat distortions.

Institute of Electrical and Electronic Engineers (IEEE)

A voluntary organization which, among other things, sponsors standards committees and is accredited by the American National Standards Institute.

International Electrotechnical Commission (IEC)

An international standards body.

International Organization for Standardization (ISO)

An international standards body, commonly known as the International Standards Organization.

Internet Control Message Protocol (ICMP)

An Internet network-layer protocol.

Internet Engineering Task Force (IETF)

A body responsible, among other things, for developing standards used in the Internet.

Internet Group Management Protocol (IGMP)

A network-layer protocol for managing multicast groups on the Internet.

Impulse Noise

Noise characterized by non-overlapping transient disturbances.

Information Element

The fields that make up a MAP and define individual grants, deferred grants, etc.

Internet Protocol (IP)

An Internet network-layer protocol.

Interval Usage Code

A field in MAPs and UCDs to link burst profiles to grants.

Latency

The time, expressed in quantity of symbols, taken for a signal element to pass through a device.

Layer

A subdivision of the Open System Interconnection (OSI) architecture, constituted by subsystems of the same rank.

Link Layer

See Data Link Layer.

Local Area Network (LAN)

A non-public data network in which serial transmission is used for direct data communication among data stations located on the user's premises.

Logical Link Control (LLC) procedure

In a local area network (LAN) or a Metropolitan Area Network (MAN), that part of the protocol that governs the assembling of data link layer frames and their exchange between data stations, independent of how the transmission medium is shared.

Logical (Upstream) Channel

A MAC entity identified by a unique channel ID and for which bandwidth is allocated by an associated MAP message. A physical upstream channel may support multiple logical upstream channels. The associated UCD and MAP messages completely describe the logical channel.

MAC Frame

MAC header plus optional PDU.

MAC Service Access Point

An attachment to a MAC-sublayer domain.

MAP

See Bandwidth Allocation Map.

Master Head-End

A head-end which collects television program material from various sources by satellite, microwave, fiber and other means, and distributes this material to Distribution Hubs in the same metropolitan or regional area. A Master Head-End MAY also perform the functions of a Distribution Hub for customers in its own immediate area.

Mean Time to Repair (MTTR)

In cable television systems, the MTTR is the average elapsed time from the moment a loss of RF channel operation is detected up to the moment the RF channel operation is fully restored.

Media Access Control (MAC) address

The “built-in” hardware address of a device connected to a shared medium.

Media Access Control (MAC) procedure

In a subnetwork, that part of the protocol that governs access to the transmission medium independent of the physical characteristics of the medium, but taking into account the topological aspects of the subnetworks, in order to enable the exchange of data between nodes. MAC procedures include framing, error protection, and acquiring the right to use the underlying transmission medium.

Media Access Control (MAC) sublayer

The part of the data link layer that supports topology-dependent functions and uses the services of the Physical Layer to provide services to the logical link control (LLC) sublayer.

Micro-reflections

Echoes in the forward transmission path due to departures from ideal amplitude and phase characteristics.

Mid Split

A frequency division scheme that allows bi-directional traffic on a single coaxial cable. Reverse channel signals propagate to the head-end from 5 to 108 MHz. Forward path signals go from the head-end from 162 MHz to the upper frequency limit. The duplex crossover band is located from 108 to 162 MHz.

Mini-Slot

A “mini-slot” is an integer multiple of 6.25-microsecond increments.

Modulation Rate

The signaling rate of the upstream modulator (1280 to 5120 kHz). In S-CDMA, the chip rate. In TDMA, the channel symbol rate.

Moving Picture Experts Group (MPEG)

A voluntary body which develops standards for digital compressed moving pictures and associated audio.

Multipoint Access

User access in which more than one terminal equipment is supported by a single network termination.

Multipoint Connection

A connection among more than two data network terminations.

National Cable & Telecommunications Association (NCTA)

A voluntary association of cable television operators which, among other things, provides guidance on measurements and objectives for cable television systems in the USA.

National Television Systems Committee (NTSC)

Committee which defined the analog color television broadcast standard used today in North America.

Network Layer

Layer 3 in the Open Systems Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.

Network Management

The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.

Number Of Allocated Codes

The total number of codes which a single CM uses in a single S-CDMA frame. This number is determined by the size of the grants in minislots and the mapping of these minislots to S-CDMA frames (note that a CM may receive multiple grants which are mapped to a single S-CDMA frame). The number of allocated codes can be in the range of the number of Codes per Mini-slot to the number of active codes, and may vary from frame to frame, but is constant within an S-CDMA frame.

Open Systems Interconnection (OSI)

A framework of ISO standards for communication between different systems made by different vendors, in which the communications process is organized into seven different categories that are placed in a layered sequence based on their relationship to the user. Each layer uses the layer immediately below it and provides a service to the layer above. Layers 7 through 4 deal with end-to-end communication between the message source and destination, and layers 3 through 1 deal with network functions.

Organizationally Unique Identifier (OUI)

A 3-octet IEEE assigned identifier that can be used to generate Universal LAN MAC addresses and Protocol Identifiers per ANSI/IEEE Std 802 for use in Local and Metropolitan Area Network applications.

Packet Identifier (PID)

A unique integer value used to identify elementary streams of a program in a single- or multi-program MPEG-2 stream.

Partial Grant

A grant that is smaller than the corresponding bandwidth request from the CM.

Payload Header Suppression

The suppression of the header in a payload packet. (e.g., the suppression of the Ethernet header in forwarded packets).

Payload Unit Start Indicator (PUSI)

A flag in an MPEG header. A value of 1 indicates the presence of a pointer field as the first byte of the payload.

Physical (PHY) Layer

Layer 1 in the Open System Interconnection (OSI) architecture; the layer that provides services to transmit bits or groups of bits over a transmission link between open systems and which entails electrical, mechanical and handshaking procedures.

Physical Media Dependent (PMD) Sublayer

A sublayer of the Physical Layer which is concerned with transmitting bits or groups of bits over particular types of transmission link between open systems and which entails electrical, mechanical and handshaking procedures.

Primary Service Flow

All CMs have a Primary Upstream Service Flow and a Primary Downstream Service Flow. They ensure that the CM is always manageable and they provide a default path for forwarded packets that are not classified to any other Service Flow.

Program-Specific Information (PSI)

In MPEG-2, normative data necessary for the demultiplexing of Transport Streams and the successful regeneration of programs.

Program Stream

In MPEG-2, a multiplex of variable-length digital video and audio packets from one or more program sources having a common time-base.

Protocol

A set of rules and formats that determines the communication behavior of layer entities in the performance of the layer functions.

Provisioned Service Flow

A Service Flow that has been provisioned as part of the Registration process, but has not yet been activated or admitted. It may still require an authorization exchange with a policy module or external policy server prior to admission.

QoS Parameter Set

The set of Service Flow Encodings that describe the Quality of Service attributes of a Service Flow or a Service Class.

Quadrature Amplitude Modulation (QAM)

A method of modulating digital signals onto a radio-frequency carrier signal involving both amplitude and phase coding.

Quadrature Phase-Shift Keying (QPSK)

A method of modulating digital signals onto a radio-frequency carrier signal using four phase states to code two digital bits.

Radio Frequency (RF)

In cable television systems, this refers to electromagnetic signals in the range 5 to 1000 MHz.

Reference Code Matrix

A 128-by-128 element matrix formed by stacking successive spreading codes on top of each other, i.e., the bottom row of the reference code matrix is Code 0 (all ones) and the top row is Code 127. The code elements are placed in the matrix from right to left, i.e., the right-most column of the code matrix is the first element of each code, and the left-most column is the last element of each code.

Request For Comments (RFC)

A technical policy document of the IETF; these documents can be accessed on the World Wide Web at <http://www.rfc-editor.org/>.

Return Loss

The parameter describing the attenuation of a guided wave signal (e.g., via a coaxial cable) returned to a source by a device or medium resulting from reflections of the signal generated by the source.

Reverse Channel

The direction of signal flow towards the head-end, away from the subscriber; equivalent to Upstream.

Routing Information Protocol (RIP)

A protocol of the IETF for exchanging routing information about IP networks and subnets.

S-CDMA Frame

A two dimensional representation of mini-slots, where the dimensions are codes and time. An S-CDMA frame is composed of p active codes in the code dimension and K spreading intervals in the time dimension. Within the S-CDMA frame, the number of mini-slots is determined by the number of codes per mini-slot (c) and p , the number of active codes in the S-CDMA frame. Each S-CDMA frame thus contains s mini-slots, where $s=p/c$, and each mini-slot contains $c*K$ information (QAM) symbols.

S-CDMA Subframe

A subframe is a vertically-smaller subset of an S-CDMA frame over which interleaving is performed, where the vertical dimension is R' codes, where $R' \leq p$ (the number of active codes). A subframe is generally used to constrain the interleaving region to be of a similar size to the Reed-Solomon codeword in order to provide protection from impulse noise.

Security Association Identifier

A Baseline Privacy security identifier between a CMTS and a CM.

Service Access Point (SAP)

The point at which services are provided by one layer, or sublayer to the layer immediately above it.

Service Class

A set of queuing and scheduling attributes that is named and that is configured at the CMTS. A Service Class is identified by a Service Class Name. A Service Class has an associated QoS Parameter Set.

Service Class Name

An ASCII string by which a Service Class may be referenced in modem configuration files and protocol exchanges.

Service Data Unit (SDU)

Information that is delivered as a unit between peer service access points.

Service Flow A MAC-layer transport service which:

- Provides unidirectional transport of packets from the upper layer service entity to the RF;
- Shapes, polices, and prioritizes traffic according to QoS traffic parameters defined for the Flow.

Service Flow Identifier (SFID)

An identifier assigned to a service flow by the CMTS. [32 bits].

Service Flow Reference

A message parameter in Configuration Files and Dynamic Service MAC messages used to associate Classifiers and other objects in the message with the Service Flow Encodings of a requested Service Flow.

Service Identifier (SID)

A Service Flow Identifier assigned by the CMTS (in addition to a Service Flow Identifier) to an Active or Admitted Upstream Service Flow. [14 bits]

Simple Network Management Protocol (SNMP)

A network management protocol of the IETF.

Spectrum Management System (SMS)

A system, defined in [SMS], for managing the RF cable spectrum.

Spread Symbol Or Spreading Interval

At the output of the spreader, a group of 128 chips which comprise a single S-CDMA spreading code, and are the result of spreading a single information (QAM) symbol. One spread symbol = one spreading interval = 128 chips = one information (QAM) symbol.

Spreader-Off S-CDMA Burst

A transmission from a single CM in a spreader-off frame on an S-CDMA channel defined by the time in which the CM's transmitter turns on to the time it turns off. There will generally be several spreader off bursts in a spreader-off frame.

Spreader-Off S-CDMA Frame

TDMA mini-slots on an S-CDMA channel in which the spreader is turned off. These are differentiated from TDMA bursts on a TDMA channel in that, for example, the number of mini-slots per spreader-off SCDMA burst frame is constrained to be the same as the number of mini-slots in a spreader-on SCDMA frame (s). This number of mini-slots will be less than the number of TDMA mini-slots in a TDMA channel over the same time interval if the number of active codes is significantly less than 128.

Spreading Interval

Time to transmit a single complete S-CDMA spreading code, equal to the time to transmit 128 chips. Also, time to transmit a single information (QAM) symbol on an S-CDMA channel. See also Spread Symbol.

Sub-Channel

A logical channel sharing same upstream spectrum (RF center frequency and RF channel) with other logical channels.

Sublayer

A subdivision of a layer in the Open System Interconnection (OSI) reference model.

Subnetwork

Subnetworks are physically formed by connecting adjacent nodes with transmission links.

Subnetwork Access Protocol (SNAP)

An extension of the LLC header to accommodate the use of 802-type networks as IP networks.

Subscriber

See End User.

Subsplit

A frequency-division scheme that allows bi-directional traffic on a single cable. Reverse path signals come to the head-end from 5 to 30 (up to 42 on Extended Subsplit systems) MHz. Forward path signals go from the head-end from 50 or 54 MHz to the upper frequency limit of the cable network.

Subsystem

An element in a hierarchical division of an Open System that interacts directly with elements in the next higher division or the next lower division of that open system.

System Clock Period

The period of the 10.24 MHz system clock, nominally 97.65625 ns.

Systems Management

Functions in the application layer related to the management of various open systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.

Tick

6.25-microsecond time intervals that are the reference for upstream mini-slot definition and upstream transmission times.

Tilt

Maximum difference in transmission gain of a cable television system over a given bandwidth (typically the entire forward operating frequency range).

Transit Delay

The time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.

Transmission Control Protocol (TCP)

A transport-layer Internet protocol which ensures successful end-to-end delivery of data packets without error.

Transmission Convergence Sublayer

A sublayer of the Physical Layer that provides an interface between the Data Link Layer and the PMD Sublayer.

Transmission Link

The physical unit of a subnetwork that provides the transmission connection between adjacent nodes.

Transmission Medium

The material on which information signals may be carried; e.g., optical fiber, coaxial cable, and twisted-wire pairs.

Transmission System

The interface and transmission medium through which peer physical layer entities transfer bits.

Transmit On/Off Ratio

In multiple-access systems, the ratio between the signal powers sent to line when transmitting and when not transmitting.

Transport Stream

In MPEG-2, a packet-based method of multiplexing one or more digital video and audio streams having one or more independent time bases into a single stream.

Trivial File-Transfer Protocol (TFTP)

An Internet protocol for transferring files without the requirement for user names and passwords that is typically used for automatic downloads of data and software.

Trunk Cable

Cables that carry the signal from the head-end to groups of subscribers. The cables can be either coaxial or fiber depending on the design of the system.

Type/Length/Value (TLV)

An encoding of three fields, in which the first field indicates the type of element, the second the length of the element, and the third field the value.

Upstream

The direction from the subscriber location toward the head-end.

Upstream Channel Descriptor (UCD)

The MAC Management Message used to communicate the characteristics of the upstream physical layer to the cable modems.

4 ABBREVIATIONS

ANSI	American National Standards Institute
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BPDU	Bridge Protocol Data Unit
BPI	Baseline Privacy Interface
CA	Certificate Authority
CATV	Community Access Television, Cable Television
CCCM	CPE Controlled Cable Modem
CM	Cable Modem
CMCI	Cable Modem to CPE Interface
CMTS	Cable Modem Termination System
CMTS-NSI	Cable Modem Termination System - Network Side Interface
CPE	Customer Premises Equipment
CSA	Code Signing Agent
CVC	Code Verification Certificate
DCC	Dynamic Channel Change
DES	Digital Encryption Standard
DH	Diffie-Helman
DHCP	Dynamic Host Configuration Protocol
DOCSIS 1.x	Abbreviation for “DOCSIS 1.0 or 1.1”
DOCSIS	Data-Over-Cable Service Interface Specifications
ECN	Engineering Change Notice
ECO	Engineering Change Order
ECR	Engineering Change Request
FDDI	Fiber Distributed Data Interface
FTP	File Transfer Protocol
HFC	Hybrid Fiber/Coax (HFC) System
ICMP	Internet Control Message Protocol
IE	Information Element
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCDN	Internet Protocol over Cable Data Network (IETF working group)

IPDR	Internet Protocol Detail Record
IUC	Interval Usage Code
LAN	Local Area Network
LLC	Logical Link Control procedure
MAC	Media Access Control procedure
MIB	Management Information Base
MPEG	Moving Picture Experts Group
MSAP	MAC Service Access Point
MSO	Multiple System Operator
MTA	Multimedia Terminal Adapter
NMS	Network Management System
OID	Object Identifier
OSI	Open Systems Interconnection
OSSI	Operations Support System Interface
OUI	Organization Unique Identifier
PCI	Peripheral Component Interconnect
PDU	Payload Data Unit
PHS	Payload Header Suppression
PHY	Physical (PHY) Layer
PID	Packet Identifier
PMD	Physical Media Dependent (PMD) Sublayer
PSI	Program-Specific Information
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RFC	Request for Comments
RFI	Radio Frequency Interface
RO	Read Only
RW	Read/Write
SAID	Security Association Identifier
SCN	Service Class Name
SF	Service Flow
SFID	Service Flow Identifier
SID	Service Identifier
SLA	Service Level Agreement
SMI	Structure of Management Information
SMS	Spectrum Management System

SNAP	Subnetwork Access Protocol
SNMP	Simple Network Management Protocol
SNMPv1	Version 1 of the Simple Network Management Protocol
SNMPv2c	Version 2C of the Simple Network Management Protocol
SNMPv3	Version 3 of the Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File-Transfer Protocol
TLV	Type/Length/Value
UCC	Upstream Channel Change
UDP	User Datagram Protocol
USB	Universal Synchronous Bus
USM	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol
VACM	View-based Access Control Model for the simple Network Management Protocol (SNMP)
VoIP	Voice over Internet Protocol
XML	Extensible Markup Language

5 SNMP PROTOCOL

The SNMPv3 protocol has been selected as the communication protocol for management of data-over-cable services and MUST be implemented. Although SNMPv3 offers advantages, many management systems may not be capable of supporting SNMPv3 agents; therefore, support of SNMPv1 and SNMPv2c is also required and MUST be implemented.

The following IETF SNMP-related RFCs MUST be implemented:

[RFC 3410]	Introduction and Applicability Statements for Internet Standard Management Framework
[RFC 3411]	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
[RFC 3412]	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
[RFC 3413]	Simple Network Management Protocol (SNMP) Applications
[RFC 3414]	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
[RFC 3415]	View-based Access Control Model (VACM) for the simple Network Management Protocol (SNMP)
[RFC 3416]	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
[RFC 3417]	Transport Mappings for the Simple Network Management Protocol (SNMP)
[RFC 3418]	Management Information Base for the Simple Network Management Protocol (SNMP)
[RFC 2576]	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
[RFC 1901]	Introduction to Community-based SNMPv2 (Informational)
[RFC 1157]	A Simple Network Management Protocol

For support of SMIV2, the following IETF SNMP-related RFCs MUST be implemented:

[RFC 2578]	Structure of Management Information Version 2 (SMIV2)
[RFC 2579]	Textual Conventions for SMIV2
[RFC 2580]	Conformance Statements for SMIV2

For support of Diffie-Helman Key exchange for the User Based Security Model, the following IETF SNMP RFC MUST be implemented:

[RFC 2786]	Diffie-Helman USM Key Management Information Base and Textual Convention
------------	--

5.1 SNMP Mode for DOCSIS 2.0-compliant CMTSes

DOCSIS 2.0-compliant CMTSes MUST support SNMPv1, SNMPv2c, and SNMPv3 and SNMP coexistence as described by [RFC 3411] through [RFC 3415] and [RFC 2576], and MAY support SNMPv1 and SNMPv2c vendor proprietary solutions, including SNMP v1/v2c NmAccess mode, with the following requirements:

- a) DOCSIS 2.0 compliant CMTS MUST operate in SNMP coexistence mode (not using docsDevNmAccessTable); additionally, SNMP coexistence mode MAY be disabled, by vendor proprietary configuration control, to allow the CMTS to support SNMPv1, SNMPv2c vendor proprietary solutions, including SNMP v1/v2c NmAccess mode (using docsDevNmAccessTable).

- b) CMTSes in SNMPv1/v2c NmAccess mode (using DOCS-CABLE-DEVICE-MIB docsDevNmAccessTable) MUST operate subject to the following requirements and limitations:
- Only SNMPv1/v2c packets are processed.
 - SNMPv3 packets are dropped [RFC 2669].
 - The docsDevNmAccessTable controls SNMP access and SNMP trap destinations as described in [RFC 2669].
 - None of the SNMPv3 MIBs as defined in [RFC 3411] through [RFC 3415] and [RFC 2576] are accessible.
- c) CMTS SNMPv1, SNMPv2c vendor-proprietary solutions MUST operate subject to the following requirements and limitations:
- Only SNMPv1/v2c packets are processed.
 - SNMPv3 packets are dropped.
 - Vendor-proprietary solutions MUST control SNMP access and SNMP trap destinations.
 - None of the SNMPv3 MIBs as defined in [RFC 3411] through [RFC 3415] and [RFC 2576] are accessible.
- d) CMTS SNMP Coexistence Mode MUST operate subject to the following requirements and limitations:
- SNMP v1/v2c/v3 Packets are processed as described by in [RFC 3411] through [RFC 3415] and [RFC 2576].
 - docsDevNmAccessTable is not accessible. (If the CMTS also support DOCS-CABLE-DEVICE-MIB).
 - Access control and trap destinations are determined by the SNMP-COMMUNITY-MIB, SNMP-NOTIFICATION-MIB, SNMP-TARGET-MIB, SNMP-VIEW-BASED-ACM-MIB, SNMP-COMMUNITY-MIB, and SNMP-USER-BASED-SM-MIB.
 - The SNMP-COMMUNITY-MIB controls the translation of SNMPv1/v2c packet community string into securityName which select entries in the SNMP-USER-BASED-SM-MIB. Access control is provided by the SNMP-VIEW-BASED-ACM-MIB.
 - The SNMP-USER-BASED-SM-MIB and SNMP-VIEW-BASED-ACM-MIB control SNMPv3 packets.
 - Trap destinations are specified in the SNMP-TARGET-MIB and SNMP-NOTIFICATION-MIB.

5.1.1 Key Change Mechanism

DOCSIS 2.0-compliant CMTSes SHOULD use the key-change mechanism specified in [RFC 2786]. CMTSes MUST always support the key-change mechanism described in [RFC 3414] to comply with the industry wide SNMPv3 standard.

5.2 SNMP Mode for DOCSIS 2.0-compliant CMs

DOCSIS 2.0-compliant CMs (in 2.0, 1.1, and 1.0 modes) MUST support SNMPv1, SNMPv2c, and SNMPv3 as well as SNMP-coexistence ([RFC 2576]) subject to the following requirements:

- a) Before completion of registration, the CM MUST operate as follows (in some CCCM implementations, SNMP access MAY be made inaccessible from the CPE for security reasons; in such implementation, the access to similar set of MIB objects SHOULD be provided by a diagnostic utility as described in Section 9.3):
- IP connectivity between the CM and the SNMP management station MUST be implemented as described in Section 9.1.

- The CM MUST provide read-only access to the following MIB objects:
docsIfDownChannelFrequency
docsIfDownChannelPower
docsIfCmStatusValue
docsDevServerBootState
docsDevEventTable.
 - The CM MAY provide read-only access to the following MIB objects:
sysDescr
sysUptime
ifTable
ifXtable
docsIfUpChannelFrequency
docsIfSigQSignalQualityTable
docsIfCmCmtsAddress
docsIfCmStatusTxPower
docsDevSwCurrentVers.
 - The CM MAY provide access to additional information, but MUST NOT reveal:
CoS and QoS service flow information
configuration file contents
Secure Software Download information
Key authentication and encryption material
SNMP management and control
DOCSIS functional modules statistics and configuration
Network provisioning hosts and servers IPs addresses.
 - Access from the RF interface MUST NOT be allowed.
 - SNMPv1/v2c packets are accepted which contain any community string.
 - All SNMPv3 packets are dropped.
 - The registration request MUST be sent and registration MUST be completed after successful processing of all MIB elements in the config file, but before beginning the calculation of the public values in the USMDHKickstart Table.
- b) The content of the CM config file determines the CM SNMP mode after registration.
- CM is in SNMPv1/v2c docsDevNmAccess mode if the CM configuration file contains ONLY docsDevNmAccessTable setting for SNMP access control.
 - If the configuration file does not contain SNMP access control items (docsDevNmAccessTable or snmpCommunityTable or TLV 34.1/34.2 or TLV38), the CM is in NmAccess mode.
 - CM is in SNMP coexistence mode if the CM configuration file contains snmpCommunityTable setting and/or TLV type 34.1 and 34.2 and/or TLV type 38. In this case, any entries made to the docsDevNmAccessTable are ignored.
- c) After completion of registration, the modem operates in one of 2 modes. The operating mode is determined by the contents of the config file as described above.

SNMPv1/v2c NmAccess Mode (using docsDevNmAccess Table)

- Only SNMPv1/v2c packets are processed.
- SNMPv3 packets are dropped.
- docsDevNmAccessTable controls access and trap destinations as described in [RFC 2669].
- None of the SNMPv3 MIBs as defined in [RFC 3411] through [RFC 3415] and [RFC 2576] are accessible.

SNMP Coexistence Mode

During calculation of USMDHKickstartTable public values:

- The modem **MUST NOT** allow any SNMP access from the RF port.
- The modem **MAY** continue to allow access from the CPE port with the limited access as configured by the SNMP-COMMUNITY-MIB, SNMP-TARGET-MIB, SNMP-VIEW-BASED-ACM-MIB and SNMP-USER-BASED-SM-MIB.

After calculation of USMDHKickstartTable public values:

- The modem **MUST** send the cold start or warm start trap to indicate that the modem is now fully SNMPv3 manageable.
 - SNMP V1/V2c/V3 Packets are processed as described by [RFC 3411] through [RFC 3415] and [RFC 2576].
 - docsDevNmAccessTable is not accessible.
 - Access control and trap destinations are determined by the SNMP-COMMUNITY-MIB, SNMP-NOTIFICATION-MIB, SNMP-TARGET-MIB, SNMP-VIEW-BASED-ACM-MIB, SNMP-COMMUNITY-MIB, and SNMP-USER-BASED-SM-MIB.
 - The SNMP-COMMUNITY-MIB controls the translation of SNMPv1/v2c packet community string into security name which select entries in the SNMP-USER-BASED-SM-MIB. Access control is provided by the SNMP-VIEW-BASED-ACM-MIB.
 - SNMP-USER-BASED-SM-MIB and SNMP-VIEW-BASED-ACM-MIB controls SNMPv3 packets.
 - Notification destinations are specified in the SNMP-TARGET-MIB and SNMP-NOTIFICATION-MIB.
- d) In case of failure to complete SNMPv3 initialization (i.e., NMS cannot access CM via SNMPv3 PDU), the CM is in the coexistence mode and will allow SNMPv1/v2c access if and only if the SNMP-COMMUNITY-MIB entries (and related entries) are configured.

5.2.1 SNMPv3 Initialization and Key changes

DOCSIS 2.0-compliant CMs **MUST** support the “SNMPv3 Initialization” and “DH Key Changes” requirements specified in the following sections.

The DOCSIS 1.1 cable modem is designated as having “very-secure” security posture in the context of [RFC 3414] Annex A and [RFC 3415] Annex A. This means that default usmUser and vacmAccess entries defined in [RFC 3414] Annex A and [RFC 3415] Annex A **MUST NOT** be present.

5.2.2 SNMPv3 Initialization

For each of up to 5 different security names, the Manager generates a pair of numbers. First, the Manager generates a random number R_m .

Then, the Manager uses the DH equation to translate R_m to a public number z . The equation is as follows:

$$z = g^{R_m} \text{ MOD } p$$

where g is from the set of Diffie-Helman parameters, and p is the prime from those parameters.

The CM configuration file is created to include the (security name, public number) pair. The CM MUST support a minimum of 5 pairs. For example:

TLV type 34.1 (SNMPv3 Kickstart Security Name) = docsisManager
 TLV type 34.2 (SNMPv3 Kickstart Public Number) = z

The CM MUST support the VACM entries defined in Section 5.2.4.

During the CM boot process, the above values (security name, public number) MUST be populated in the usmDhKickstartTable.

At this point:

usmDhKickstartMgrPublic.1 = "z" (octet string)
 usmDhKickstartSecurityName.1 = "docsisManager"

When usmDhKickstartMgrPublic.n is set with a valid value during the registration, a corresponding row is created in the usmUserTable with the following values:

usmUserEngineID: localEngineID
 usmUserName: usmDhKickstartSecurityName.n value
 usmUserSecurityName: usmDhKickstartSecurityName.n value
 usmUserCloneFrom: ZeroDotZero
 usmUserAuthProtocol: usmHMACMD5AuthProtocol
 usmUserAuthKeyChange: (derived from set value)
 usmUserOwnAuthKeyChange: (derived from set value)
 usmUserPrivProtocol: usmDESPrivProtocol
 usmUserPrivKeyChange: (derived from set value)
 usmUserOwnPrivKeyChange: (derived from set value)
 usmUserPublic
 usmUserStorageType: permanent
 usmUserStatus: active

Note: For (CM) dhKickstart entries in usmUserTable, Permanent means it MUST be written to but not deleted and is not saved across reboots.

After the CM has registered with the CMTS:

1. The CM generates a random number x_a for each row populated in the usmDhKickstartTable which has a non-zero length usmDhKickstartSecurityName and usmDhKickstartMgrPublic.
2. The CM uses DH equation to translate x_a to a public number c (for each row identified above).

$c = g^{x_a} \text{ MOD } p$
 where g is the from the set of Diffie-Helman parameters, and p is the prime from those parameters

At this point:

usmDhKickstartMyPublic.1 = "c" (octet string)
 usmDhKickstartMgrPublic.1 = "z" (octet string)
 usmDhKickstartSecurityName.1 = "docsisManager"

3. The CM calculates shared secret sk where $sk = z^{x_a} \text{ mod } p$.

4. The CM uses sk to derive the privacy key and authentication key for each row in usmDhKickstartTable and sets the values into the usmUserTable.

As specified in **[RFC 2786]**, the privacy key and the authentication key for the associated username, “docsisManager” in this case, is derived from sk by applying the key derivation function PBKDF2 defined in PKCS#5 v2.0.

```
privacy key <---PBKDF2( salt = 0xd1310ba6,
                        iterationCount = 500,
                        keyLength = 16,
                        prf = id-hmacWithSHA1 )

authentication key <----PBKDF2( salt = 0x98dfb5ac,
                                iterationCount = 500,
                                keyLength = 16 (usmHMACMD5AuthProtocol),
                                prf = id-hmacWithSHA1 )
```

At this point the CM has completed its SNMPv3 initialization process and MUST allow appropriate access level to a valid securityName with the correct authentication key and/or privacy key.

DOCSIS 2.0-compliant CMs MUST properly populate keys to appropriate tables as specified by the SNMPv3-related RFCs and [RFC 2786].

5. The following describes the process that the manager uses to derive the CM’s unique authentication key and privacy key.

The SNMP manager accesses the contents of the usmDhKickstartTable using the security name of ‘dhKickstart’ with no authentication.

DOCSIS 2.0-compliant CMs MUST provide pre-installed entries in the USM table and VACM tables to correctly create user ‘dhKickstart’ of security level noAuthNoPriv that has read-only access to system group and usmDhkickstartTable.

The SNMP manager gets the value of the CM’s usmDhKickstartMypublic number associated with the securityName for which the manager wants to derive authentication and privacy keys. Using the private random number, the manager can calculate the DH shared secret. From that shared secret, the manager can derive operational authentication and confidentiality keys for the securityName that the manager is going to use to communicate with the CM.

5.2.3 DH Key Changes

DOCSIS 2.0-compliant CMs MUST support the key-change mechanism specified in **[RFC 2786]**.

5.2.4 VACM Profile

This section addresses the default VACM profile for DOCSIS CMs operating in SNMP Coexistence mode.

The following VACM entries MUST be included by default in a compliant CM:

- The system manager, with full read/write/config access:

```
vacmSecurityModel: 3 (USM)
vacmSecurityName: docsisManager
vacmGroupName: docsisManager
vacmSecurityToGroupStorageType: permanent
vacmSecurityToGroupStatus: active
```

- An operator/CSR with read/reset access to full modem:

vacmSecurityModel: 3 (USM)
 vacmSecurityName: docsisOperator
 vacmGroupName: docsisOperator
 vacmSecurityToGroupStorageType: permanent
 vacmSecurityToGroupStatus: active

- RF Monitoring with read access to RF plant statistics:

vacmSecurityModel: 3 (USM)
 vacmSecurityName: docsisMonitor
 vacmGroupName: docsisMonitor
 vacmSecurityToGroupStorageType: permanent
 vacmSecurityToGroupStatus: active

- User debugging with read access to ‘useful’ variables:

vacmSecurityModel: 3 (USM)
 vacmSecurityName: docsisUser
 vacmGroupName: docsisUser
 vacmSecurityToGroupStorageType: permanent
 vacmSecurityToGroupStatus: active

- Group name to view translations:

vacmGroupName: docsisManager
 vacmAccessContextPrefix: “
 vacmAccessSecurityModel: 3 (USM)
 vacmAccessSecurityLevel: AuthPriv
 vacmAccessContextMatch: exact
 vacmAccessReadViewName: docsisManagerView
 vacmAccessWriteViewName: docsisManagerView
 vacmAccessNotifyViewName: docsisManagerView
 vacmAccessStorageType: permanent
 vacmAccessStatus: active

vacmGroupName: docsisOperator
 vacmAccessContextPrefix: “
 vacmAccessSecurityModel: 3 (USM)
 vacmAccessSecurityLevel: AuthPriv & AuthNoPriv
 vacmAccessContextMatch: exact
 vacmAccessReadViewName: docsisManagerView
 vacmAccessWriteViewName: docsisOperatorWriteView
 vacmAccessNotifyViewName: docsisManagerView
 vacmAccessStorageType: permanent
 vacmAccessStatus: active

vacmGroupName: docsisMonitor
 vacmAccessContextPrefix: “
 vacmAccessSecurityModel: 3 (USM)
 vacmAccessSecurityLevel: AuthNoPriv
 vacmAccessContextMatch: exact
 vacmAccessReadViewName: docsisMonitorView
 vacmAccessWriteViewName: “
 vacmAccessNotifyViewName: docsisMonitorView
 vacmAccessStorageType: permanent
 vacmAccessStatus: active

vacmGroupName: docsisUser
vacmAccessContextPrefix: ''
vacmAccessSecurityModel: 3 (USM)
vacmAccessSecurityLevel: AuthNoPriv
vacmAccessContextMatch: exact
vacmAccessReadViewName: docsisUserView
vacmAccessWriteViewName: ''
vacmAccessNotifyViewName: ''
vacmAccessStorageType: permanent
vacmAccessStatus: active

- The views:

docsisManagerView

subtree: 1.3.6.1 (Entire MIB)

docsisOperatorWriteView

subtree: docsisDevBase
subtree: docsisDevSoftware
subtree: docsisDevEvControl
subtree: docsisDevEvThrottleAdminStatus

docsisMonitorView

subtree: 1.3.6.1.2.1.1 (system)
subtree: docsisIfBaseObjects
subtree: docsisIfCmObjects

docsisUserView

subtree 1.3.6.1.2.1.1 (system)
subtree: docsisDevBase
subtree: docsisDevSwOperStatus
subtree: docsisDevSwCurrentVersion
subtree: docsisDevServerConfigFile
subtree: docsisDevEventTable
subtree: docsisDevCpeTable
subtree: docsisIfUpstreamChannelTable
subtree: docsisIfDownstreamChannelTable
subtree: docsisIfSignalQualityTable
subtree: docsisIfCmStatusTable

DOCSIS 2.0-compliant CMs MUST also support additional VACM users as they are configured via an SNMP-embedded configuration file.

6 MANAGEMENT INFORMATION BASES (MIBS)

This section defines the minimum set of managed objects required to support the management of CM and CMTS. Vendors MAY augment this MIB with objects from other standard or vendor-specific MIBs where appropriate.

The DOCSIS OSSI 2.0 specification has priority over the IETF MIBs and all objects. Though deprecated or optional in the IETF MIB, the object can be required by this specification as mandatory. Regardless of having either a status of deprecated or optional in the IETF MIB, the CM and CMTS MUST implement MIB requirements in accordance with the OSSI 2.0 specification.

If not required by this specification, deprecated objects are optional. If a CM or CMTS implements a deprecated object, the object MUST be implemented correctly according to the MIB definition. If a CM or CMTS does not implement a deprecated object, the agent MUST NOT instantiate the object and when accessed, MUST respond with the appropriate error/exception condition, such as no such object for SNMPv2c.

If not required by this specification, optional objects are optional. If a CM or CMTS implements an optional object, the object MUST be implemented correctly according to the MIB definition. If a CM or CMTS does not implement an optional object, the agent MUST NOT instantiate the object and when accessed, MUST respond with the appropriate error/exception condition, such as no such object for SNMPv2c.

If not required by this specification, obsolete objects are optional. If a CM or CMTS implements an obsolete object, the object MUST be implemented correctly according to the MIB definition. If a CM or CMTS does not implement an obsolete object, the agent MUST NOT instantiate the object and when accessed, MUST respond with the appropriate error/exception condition, such as no such object for SNMPv2c.

Section 6.1 and Section 6.2 include an overview of the MIB modules required for management of the facilities specified in the DOCSIS RFI 2.0 and BPI+ specifications.

6.1 IPCDN drafts and others

Table 6-1 - IPCDN Drafts

Reference	MIB	Applicable Device(s)
Annex J	DOCS-QOS-MIB	CM and CMTS
[IETF6]	IETF Proposed Standard RFC-version of BPI+ MIB, "draft-ietf-ipcdn-bpiplus-mib-05.txt": DOCS-BPI2-MIB	CM and CMTS
[IETF7]	IETF Proposed Standard RFC-version of USB MIB	CM only
Annex L	DOCS-SUBMGT-MIB	CMTS only
[IETF11]	IETF Proposed Standard RFC-version of RF MIB, "draft-ietf-ipcdn-docs-rfmibv2-05.txt": DOCS-IF-MIB	CM and CMTS
Annex I	DOCS-LOADBALANCING-MIB	CMTS only
Annex K	DOCS-IFEXT2-MIB	CM and CMTS

6.2 IETF RFCs

Table 6–2 - IETF RFCs

Reference	MIB	Applicable Device(s)
[RFC 2669]	DOCSIS Cable Device MIB: DOCS-CABLE-DEVICE-MIB	CM and CMTS
[RFC 2933]	Internet Group Management Protocol MIB: IGMP-STD-MIB	CM and CMTS
[RFC 2863]	The Interfaces Group MIB using SMIPv2: IF-MIB	CM and CMTS
[RFC 2665]	Ethernet Interface MIB: EtherLike-MIB	CM and CMTS
[RFC 1493]	Bridge MIB: BRIDGE-MIB	CM and CMTS
[RFC 2011]	SNMPv2 Management Information Base for the Internet Protocol using SMIPv2: IP-MIB	CM and CMTS
[RFC 2013]	Management Information Base for the User Datagram Protocol using SMIPv2: UDP-MIB	CM and CMTS
[RFC 3418]	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP): SNMPv2-MIB	CM and CMTS
[RFC 3410] [RFC 3411] [RFC 3412] [RFC 3413] [RFC 3414] [RFC 3415] [RFC 2576]	SNMP v3 MIBs: SNMP-FRAMEWORK-MIB, SNMP-MPD-MIB, SNMP-NOTIFICATION-MIB, SNMP-TARGET-MIB, SNMP-USER-BASED-SM-MIB, SNMP-VIEW-BASED-ACM-MIB, SNMP-COMMUNITY-MIB	CM and CMTS
[RFC 2786]	RFC-2786: Diffie-Helman USM Key: SNMP-USM-DH-OBJECTS-MIB	CM and CMTS

6.3 Managed objects requirements

The following sections detail any additional implementation requirements for the RFCs listed. Refer to Annex A for specific object implementation requirements.

The CM and CMTS MUST support a minimum of 10 available SNMP table rows unless otherwise specified by RFC or DOCSIS specification. The CM/CMTS minimum number of available SNMP table rows SHOULD mean rows (per table) that are available to support device configuration. CM/CMTS used (default) SNMP table row entries MUST NOT apply to the minimum number of available SNMP table rows.

6.3.1 CMTS MIB requirements

DOCSIS 2.0-compliant CMTSes MUST implement the Subscriber Management MIB.

6.3.2 Requirements for [RFC 2669]

[RFC 2669] MUST be implemented by DOCSIS 2.0-compliant CMs. DOCSIS 2.0-compliant CMTSes MUST implement the mandatory required objects (as specified by Annex A), and SHOULD implement the other non-mandatory required objects.

Additional requirements affecting [RFC 2669] are also found in Section 7.3, Protocol Filters.

6.3.3 Requirements for DOCS-IF-MIB

DOCS-IF-MIB MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs. It replaces RFC 2670 for DOCSIS 2.0.

The docsIfDownChannelPower object-type MUST be implemented in a CMTS that provides an integrated RF up-converter. If the CMTS relies on an external up-converter, then the CMTS SHOULD implement the docsIfDownChannelPower object-type. The CMTS transmit power reported in the MIB object MUST be within 2 dB of the actual transmit power in dBmV when implemented. If transmit power management is not implemented, the MIB object will be read-only and report the value of 0 (zero).

The docsIfDownChannelPower object-type MUST be implemented in DOCSIS 2.0-conforming CMs. This object is read-only. When operated at nominal line-voltage, at normal room temperature, the reported power MUST be within 3 dB of the actual received channel power.

For modems built based on the multi-programme television distribution used in North-America, for any 1 dB change in input power the CM MUST report a power change in the same direction that is not less than 0.5 dB and not more than 1.5 dB across the input power range from -15 dBmV to +15 dBmV.

For modems built based on the European multi-programme television distribution (Euro-DOCSIS), for any 1 dB change in input power the CM MUST report a power change in the same direction that is not less than 0.5 dB and not more than 1.5 dB across the input power range from -13 dBmV to +17 dBmV when a 256QAM downstream signal is used, and across the input power range from -17 dBmV to +13 dBmV when a 64QAM downstream signal is used.

The access of docsIfDownChannelFrequency object MUST be implemented as RW if a CMTS is in control of the downstream frequency. But if a CMTS provides IF output, docsIfDownChannelFrequency MUST be implemented as read-only and return 0.

The docsIfQosProfMaxTransmitBurst range MUST be the same as the one defined in the RFIv2.0 specification, Section C.1.1.4.6 “Maximum Upstream Channel Transmit Burst Configuration Setting” which has range 0 to 65535.

In order to be considered a valid modulation profile for assignment to an upstream channel, all entries (IUCs) in the modulation profile MUST have the same value of docsIfCmtsModChannelType. When assigning a modulation profile to an upstream channel, the value of docsIfUpChannelType and the value of docsIfCmtsModChannelType MUST match.

If a modulation profile is in use by one or more upstream channels, the value of docsIfCmtsModChannelType MUST NOT be changed. If a modulation profile is in use by one or more upstream channels, it docsIfCmtsModControl MUST NOT be set to ‘destroy’ or ‘notInService’. Before destroying a modulation profile, or changing the value of docsIfCmtsModChannelType for a profile, the user will need to ensure that it is not currently in use by any upstream channel.

The maximum number of modulation profiles that a CMTS can support in docsIfCmtsModulationTable is vendor-specific.

The CMTS MAY provide pre-defined modulation profiles (entries in the DOCS-IF-MIB docsIfCmtsModulationTable) for the purpose of being used by operators directly or as templates to define other modulation profiles. The pre-defined modulation profiles provided by the CMTS MAY be read-only to prevent users from accidental modifications. It should be noted that adding or creating entries with new docsIfCmtsModIntervalUsageCode values and the same docsIfCmtsModIndex value as a pre-defined modulation profile MAY result in an error.

The modulation profiles are PHY layer specific. Modulation profiles with the same value of docsIfCmtsModIndex may not be optimal for all upstream channels with different physical layer hardware. As a result, re-using modulation profiles for upstream channels with different physical layer hardware could decrease upstream performance. Therefore, SNMP set operations MAY result in an error when modulation profiles with the same value of docsIfCmtsModIndex are assigned to upstream channels with different physical layer hardware.

If the CMTS implements the docsIfUpChannelStatus object-type, the CMTS MUST NOT allow it to be set from active(1) directly or indirectly to destroy(6). The CMTS MUST return a wrongValue error. Entries with

docsIfUpChannelStatus set to active(1) are logically linked to a physical interface, not temporarily created to clone parameters.

The CMTS MUST support the ability to configure upstream and downstream channel IDs via the DOCS-IF-MIB. To support this ability, the MIB object docsIfDownChannelId MUST be read-write and docsIfUpChannelId MUST be read-create on the CMTS. Note that the configuration of channel IDs is expected to take place prior to any modems being present on those channels, as it is likely that any CMs that are already online will re-initialize and/or attempt to use a channel other than the one intended. The CMTS MUST ensure that an upstream or downstream channel ID is unique within a MAC-Sublayer domain.

The CMTS MUST support the objects in the docsIfCmtsUpChannelCounterTable that are described in the DOCS-IF-MIB as being optional. Note however that certain impairment events on the upstream channel (e.g., burst noise) could be indistinguishable from collisions, and hence, may be counted as such.

6.3.4 Requirements for [RFC 2863]

[RFC 2863] MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs.

The CMTS/CM ifAdminStatus object MUST provide administrative control over both MAC interfaces and individual channel and MUST be implemented as RW.

The ifType object has been assigned the following enumerated values for each instance of a Data Over Cable Service (DOCS) interface:

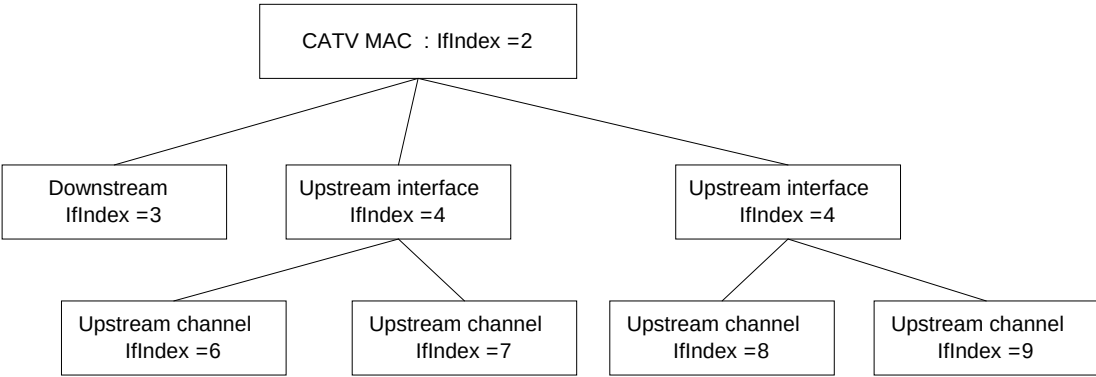
CATV MAC interface: docsCableMacLayer (127)
CATV downstream channel: docsCableDownstream (128)
CATV upstream interface: docsCableUpStream (129)
CATV upstream logical channel: docsCableUpstreamChannel (205)

6.3.4.1 Interface organization and numbering

Assigned interface numbers for CATV-MAC and Ethernet (Ethernet-like interface) are used in both the NMAccessTable and IP/LLC filtering table to configure access and traffic policy at these interfaces. These configurations are generally encoded in the configuration file using TLV encoding. To avoid provisioning complexity the interface-numbering scheme MUST comply with the following requirements:

- A CM supports only one upstream interface. At the CM, an instance of IfEntry MUST exist for each CATV-MAC interface, downstream channel, upstream interface, and each LAN interface enabled. The enabling of LAN interfaces MAY be fixed a priori during the manufacturing process or MAY be determined dynamically during operation by the CM according to whether or not an interface has a CPE device attached to it.
- If the CM has multiple CPE interfaces but only one CPE interface can be enabled at any given time, the ifTable MUST contain only the entry corresponding to the enabled or the default CPE interface. If a MAC interface consists of more than one upstream and downstream channel, a separate instance of ifEntry MUST exist for each channel.
- A 2.0 CMTS supports more than one upstream logical channel per upstream interface. At the CMTS, an instance of IfEntry MUST exist for each CATV-MAC interface, downstream channel, upstream interface, upstream logical channel, and any other interface enabled.
- For CM/CMTS, the ifStack group ([RFC 2863]) must be implemented to identify relationships among sub-interfaces. Note that the CATV-MAC interface MUST exist, even though it is broken out into sub-interfaces.

The following example illustrates a MAC interface with one downstream, two upstream interfaces each with two upstream logical channels for a CMTS.

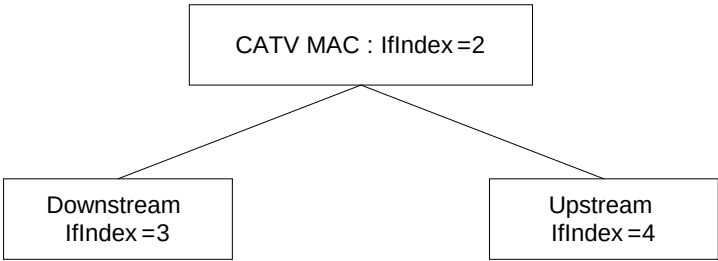


Implementation of ifStackTable for this example :

ifStackHigherLayer	ifStackLowerLayer
0	2
2	3
2	4
2	5
3	0
4	9
4	7
5	9
5	9
6	0
7	0
8	0
9	0

Figure 6-1 - ifIndex example for CMTS

The following example illustrates a MAC interface with one downstream and one upstream interface for a CM.



Implementation of ifStackTable for this example :

ifStackHigherLayer	ifStackLowerLayer
0	2
2	3
2	4
3	0
4	0

Figure 6-2 - ifIndex example for CM

At the CMTS, interface number is at the discretion of the vendor, and SHOULD correspond to the physical arrangement of connections. If table entries exist separately for upstream and downstream channels, then the ifStack group (**[RFC 2863]**) MUST be implemented to identify the relationship among sub-interfaces. Note that the CATV MAC interface(s) MUST exist, even if further broken out into sub-interfaces.

At the CM, interfaces MUST be numbered as follows:

Table 6–3 - CM interface numbering

Interface	Type
1	Primary CPE interface
2	CATV-MAC
3	RF-down
4	RF-up
5 - 15, 32 +n	Other interfaces
16 - 31	Other interfaces (Reserved)

If the CM has more than one CPE interface, the vendor MUST define which of the n CPE interfaces is the primary CPE interface. The definition of the primary CPE interface MAY be fixed a priori during manufacturing process or MAY be determined dynamically during operation by the CM according to which interface has a CPE device attached to it. Regardless of the number of CPE interfaces the CM has, or how the primary CPE interface is defined, the primary interface MUST be interface number 1.

The definition of the secondary CPE interface MAY be fixed a priori during manufacturing process or MAY be determined dynamically during operation by the CM according to which interface has a CPE device attached to it. The secondary CPE, and other interfaces, will start at 5.

DOCSIS CMs may have multiple interfaces. If filter(s) (Ip, LLC, or NmAccess) are applied to CM IfIndex 1, the same filter(s) MUST also be applied to the “Other interfaces” (IfIndexes 5 and above); however, filters are never used to limit traffic between the CPE and “Other” interfaces within the CM.

6.3.4.2 docsIfCmStatusValue and ifOperStatus Relationship

For the CM’s RF downstream, RF upstream (upstream interface and logical channel) and RF MAC interfaces, the following are the expected relationship of ifOperStatus and docsIfCmStatusValue when ifAdminStatus = up (taken from DOCS-IF-MIB).

Table 6–4 - docsIfCmStatusValue and ifOperStatus relationship

IfOperStatus	docsIfCmStatusValue
down(2):	other(1), notReady(2)
dormant(5):	notSynchronized(3), phySynchronized(4), usParametersAcquired(5), rangingComplete(6), ipCompleet(7), todEstablished(8), paramTransferComplete(10), accessDenied(13)
up(1):	registrationComplete(11), securityEstablished(9), operational(12)

6.3.4.2.1 ifAdminStatus and traffic

If the CM and CMTS interface’s ifAdminStatus = down, the interface MUST NOT accept or forward any traffic (traffic includes data and MAC management traffic).

6.3.5 Interface MIB and Trap Enable

The Interface MIB and Trap Enable specified in **[RFC 2863]** MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs.

If a multi-layer interface model is present in the device, each sub-layer for which there is an entry in the ifTable can generate linkUp/Down traps. Since interface state changes would tend to propagate through the interface stack (from top to bottom, or bottom to top), it is likely that several traps would be generated for each linkUp/Down occurrence. The CM and CMTS MUST implement the ifLinkUpDownTrapEnable object to allow managers to control trap generation, and configure only the interface sub-layers of interest.

The default setting of ifLinkUpDownTrapEnable MUST limit the number of traps generated to one, per interface, per linkUp/Down event. Interface state changes, of most interest to network managers, occur at the lowest level of an interface stack.

On CM linkUp/Down event a trap SHOULD be generated by the CM MAC interface and not by any sub-layers of the interface. Therefore, the default setting of ifLinkUpDownTrapEnable for CM MAC MUST be set to enable, and the default setting of ifLinkUpDownTrapEnable for CM RF-Up MUST be set to disable, and the default setting of ifLinkUpDownTrapEnable for CM RF-Down MUST be set to disable.

On CMTS interfaces (MAC, RF-Downstream(s), RF-Upstream(s)) the linkUp/Down event/trap SHOULD be generated by each CMTS interface. Therefore, the default setting of ifLinkUpDownTrapEnable for each CMTS interface (MAC, RF-Downstream(s), RF-Upstream(s)) MUST be set to enable.

6.3.6 Requirements for [RFC 2665]

[RFC 2665] MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs if Ethernet or Fast Ethernet interfaces are present.

6.3.7 Requirements for [RFC 1493]

[RFC 1493] MUST be implemented by DOCSIS 2.0-compliant CMTS and CMs.

In both the CM and the CMTS (if the CMTS implements transparent bridging), the Bridge MIB (**[RFC 1493]**) MUST be implemented to manage the bridging process.

In CMTSes that implement transparent bridging, the Bridge MIB MUST be used to represent information about the MAC Forwarder states.

6.3.8 Requirements for [RFC 2011]

[RFC 2011] MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs.

6.3.8.1 The IP Group

The IP group MUST be implemented. It does not apply to IP packets forwarded by the device as a link-layer bridge. For the CM, it applies only to the device as an IP host. At the CMTS, it applies to the device as an IP host, and as a routers if IP routing is implemented.

6.3.8.2 The ICMP Group

The ICMP group MUST be implemented.

6.3.9 Requirements for [RFC 2013]

[RFC 2013] MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs.

The UDP group in [RFC 2013] MUST be implemented.

6.3.10 Requirements for [RFC 3418]

[RFC 3418] MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs.

6.3.10.1 The System Group

The System Group from [RFC 3418] MUST be implemented. See Section 7.2.1 for sysObjectID requirements.

6.3.10.2 The SNMP Group

The SNMP Group from [RFC 3418] MUST be implemented.

6.3.11 Requirements for DOCS-QOS-MIB

Annex J DOCS-QOS-MIB requirements MUST be implemented by DOCSIS 2.0 CMTSes and CMs.

6.3.12 Requirements for “draft-ietf-ipcdn-igmp-mib-01.txt”

“draft-ietf-ipcdn-igmp-mib-01.txt” requirements have been deleted for CMTSes and CMs.

6.3.13 Requirements for [RFC 2933]

[RFC 2933] MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs.

Refer to Annex E for DOCSIS 2.0 IGMP cable device implementation details.

6.3.14 Requirements for DOCS-BPI2-MIB

“draft-ietf-ipcdn-bpiplus-mib-05.txt” MUST be implemented by DOCSIS 2.0-compliant CMTSes and CMs as specified in Annex A.

Entries in the docsBpi2CmtsCACertTable that have a value for docsBpi2CmtsCACertTrust of either ‘trusted (1)’, ‘untrusted (2)’, or ‘root (4)’ MUST persist across resets for DOCSIS 2.0-compliant CMTSes. Entries with a docsBpi2CmtsCACertTrust value of ‘chained (3)’ MAY persist across resets. The CMTS MUST be capable of removing entries in the docsBpi2CmtsCACertTable via SNMP by setting the row status to ‘destroy’. New entries MUST NOT be created for certificates that already exist in the docsBpi2CmtsCACertTable.

Entries in the docsBpi2CmtsProvisionedCmCertTable MUST persist across resets for DOCSIS 2.0-compliant CMTSes. The CMTS MUST be capable of removing entries in the docsBpi2CmtsProvisionedCmCertTable via SNMP by setting the row status to ‘destroy’. New entries MUST NOT be created for certificates that already exist in the docsBpi2CmtsProvisionedCmCertTable.

6.3.15 Requirements for USB MIB

Note: Until the USB-MIB becomes an IETF RFC, the draft text will be available on the DOCSIS website.

6.3.16 Requirements for DOCS-SUBMGT-MIB

DOCSIS 2.0 compliant CMTSs MUST implement DOCS-SUBMGT-MIB, as specified in Annex L.

DOCSIS 2.0-compliant CMTSes MUST support a minimum number of thirty (30) filter groups of twenty (20) filters each.

6.3.17 Requirements for [RFC 2786]

[RFC 2786] MUST be implemented by DOCSIS 2.0-compliant CMs. [RFC 2786] MAY be implemented on the CMTS.

6.3.18 Requirements for [RFC 3083]

[RFC 3083] MUST be implemented by DOCSIS 2.0-compliant CMs as specified in Annex A.

Due to the editorial error in [RFC 3083], DOCSIS 2.0-compliant CMs MUST use the following definition for docsBpiCmAuthState and not the definition in [RFC 3083]:

```
docsBpiCmAuthState OBJECT-TYPE
SYNTAX INTEGER {
    start(1),
    authWait(2),
    authorized(3),
    reauthWait(4),
    authRejectWait(5)
}
```

MAX-ACCESS read-only

STATUS current

DESCRIPTION

"The value of this object is the state of the CM authorization FSM. The start state indicates that FSM is in its initial state."

REFERENCE

"DOCSIS Baseline Privacy Interface Specification, Section 4.1.2.1."

::= { docsBpiCmBaseEntry 3 }

In addition, compliant CMs MAY create new entries in the docsBpiCmTEKTable for any multicast SID(s) it receives in Auth-Reply messages. If implemented, the multicast SID MUST be used as an index in the docsBpiCmTEKTable in the docsIfCmServiceId field. Note that if the multicast SID is used in the docsBpiCmTEKTable, there MUST NOT be a corresponding entry in the docsIfCmServiceTable for the multicast SID, due to the definition of the docsIfCmService ID in the DOCS-IF-MIB.

6.3.19 Requirements for DOCS-IF-EXT-MIB

A DOCSIS 2.0-compliant CM/CMTS MUST NOT support the DOCS-IF-EXT MIB, which is defined in Annex G.

6.3.20 Requirements for DOCS-CABLE-DEVICE-TRAP-MIB

DOCSIS 2.0-compliant CMs and CMTSes MUST implement DOCS-CABLE-DEVICE-TRAP-MIB, as specified in Annex H.

6.3.21 Requirements for SNMPv3 MIBs

DOCSIS 2.0-compliant CMs/CMTSes MUST implement the MIBs defined in [RFC 3411] through [RFC 3415] and [RFC 2576].

For CMs, the default value for any SNMPv3 object with a storageType textual convention MUST be 'volatile(2)'. This overrides the default value specified in [RFC 3411] through [RFC 3415] and [RFC 2576]. The CM MUST only accept the value of 'volatile(2)' on any SNMPv3 storageType object. An attempted set to a value of other(1), nonVolatile(3), permanent(4), or readOnly(5) will result in an 'inconsistentValue' error. Values other than the valid range (1-5) would result in a 'wrongValue' error.

The CM and CMTS SHOULD support a minimum of 30 available rows in the vacmViewTreeFamilyTable object.

6.3.22 Requirements for DOCS-LOADBALANCING-MIB

DOCSIS 2.0-compliant CMTSes MUST implement DOCS-LOADBALANCING-MIB, as specified in Annex I.

6.3.23 Requirements for DOCS-IFEXT2-MIB

DOCSIS 2.0-compliant CM/CMTS MUST implement DOCS-IFEXT2-MIB, as specified in Annex K.

6.4 CM configuration files, TLV-11 and MIB OIDs/values

The following sections define the use of CM configuration file TLV-11 elements and the CM rules for translating TLV-11 elements into SNMP PDU (SNMP MIB OID/instance and MIB OID/instance value combinations; also referred to as SNMP varbinds).

This section also defines the CM behaviors, or state transitions, after either pass or fail of the CM configuration process.

For TLV-11 definitions refer to Annex C of [SCTE 79-1].

6.4.1 CM configuration file TLV-11 element translation (to SNMP PDU)

TLV-11 translation defines the process used by the CM to convert CM configuration file information (TLV-11 elements) into SNMP PDU (varbinds). The CM MUST translate CM configuration file TLV-11 elements into a single SNMP PDU containing (n) MIB OID/instance and value components (SNMP varbinds). Once a single SNMP PDU is constructed, the CM processes the SNMP PDU and determines the CM configuration pass/fail based on the rules for CM configuration file processing, described below. However, if a CM is not physically capable of processing a potentially large single CM configuration file-generated SNMP PDU, the CM MUST still behave as if all MIB OID/instance and value components (SNMP varbinds) from CM configuration file TLV-11 elements are processed as a single SNMP PDU.

In accordance with [RFC 3416], the single CM configuration file generated SNMP PDU will be treated "as if simultaneous" and the CM must behave consistently, regardless of the order in which TLV-11 elements appear in the CM configuration file, or SNMP PDU.

The CM configuration file MUST NOT contain duplicate TLV-11 elements (duplicate means SNMP MIB object has identical OID). If duplicate TLV-11 elements are received by the CM, from the CM configuration file, then the CM MUST fail CM configuration.

6.4.1.1 Rules for CreateAndGo and CreateAndWait

The CM MUST support CreateAndGo for row creation.

The CM MAY support CreateAndWait, with the constraint that CM configuration file TLV-11 elements MUST NOT be duplicated (all SNMP MIB OID/instance must be unique). For instance, an SNMP PDU constructed from CM configuration file TLV-11 elements, which contains an SNMP CreateAndWait value for a given SNMP MIB OID/instance, MUST NOT also contain an SNMP Active value for the same SNMP MIB OID/instance (and vice versa). A CM configuration file MAY contain a TLV-11 CreateAndWait element if the intended result is to create an SNMP table row which will remain in the SNMP NotReady or SNMP NotInService state until a non-configuration file SNMP PDU is issued, from an SNMP manager, to update the SNMP table row status.

Both SNMP NotReady and SNMP NotInService states are valid table row states after an SNMP CreateAndWait instruction.

6.4.2 CM configuration TLV-11 elements not supported by the CM

If any CM configuration file TLV-11 elements translate to SNMP MIB OIDs that are not MIB OID elements supported by the CM, then those SNMP varbinds MUST be ignored, and treated as if they had not been present, for the purpose of CM configuration. This means that the CM will ignore SNMP MIB OIDs for other vendors' private MIBs as well as standard MIB elements that the CM does not support.

CMs that do not support SNMP CreateAndWait for a given SNMP MIB table MUST ignore, and treat as if not present, the set of columns associated with the SNMP table row.

If any CM configuration file TLV-11 element(s) are ignored, then the CM MUST report via the CM configured notification mechanism(s), after the CM is registered. The CM notification method MUST be in accordance with Section 7.4.2.3.

6.4.3 CM state after CM configuration file processing success

After successful CM configuration, via CM configuration file, the CM MUST proceed to register with the CMTS and pass data.

6.4.4 CM state after CM configuration file processing failure

If any CM configuration file generated SNMP PDU varbind performs an illegal set operation (illegal, bad, or inconsistent value) to any MIB OID/instance supported by the CM, processing of the CM configuration file MUST fail. Any CM configuration file generated SNMP PDU varbind set failure MUST cause a CM configuration failure, and the CM MUST NOT proceed with CM registration.

6.5 Treatment and interpretation of MIB counters on the CM

Octet and packet counters implemented as counter32 and counter64 MIB objects are monotonically increasing positive integers with no specific initial value and a maximum value based on the counter size that will roll-over to zero when it is exceeded. In particular, counters are defined such that the only meaningful value is the difference between counter values as seen over a sequence of counter polls. However, there are two situations that can cause this consistent monotonically increasing behavior to change: 1) resetting the counter due to a system or interface re initialization, or 2) a rollover of the counter when it reaches its maximum value of $2^{32}-1$ or $2^{64}-1$. In these situations, it must be clear what the expected behavior of the counters should be.

Case 1: Whenever the state of an interface changes resulting in an "interface counter discontinuity" as defined in [RFC 2863]. In this case the value of the ifXTable.ifXEntry.ifCounterDiscontinuityTime for the affected interface MUST be set to the current value of sysUpTime and ALL counters for the affected interface MUST be set to ZERO. Setting the ifAdminStatus of specified interface to down(2) MUST NOT be considered as an interface reset.

Case 2: SNMP Agent Reset. In this case, the value of the sysUpTime MUST be set to ZERO, all interface ifCounterDiscontinuityTime values MUST be set to ZERO, and all interface counters MUST be set to ZERO. Also, all other counters being maintained by the SNMP Agent MUST be set to ZERO.

Case 3: Counter Rollover. When a counter32 object reaches its maximum value of 4,294,967,295, the next value MUST be ZERO. When a counter64 object reaches its maximum value of 18,446,744,073,709,551,615, the next value MUST be ZERO. Note that unless a CM or CMTS vendor provides a means outside of SNMP to preset a counter64 or counter32 object to an arbitrary value, it will not be possible to test any rollover scenarios for counter64 objects (and many counter32 objects as well). This is because it is not possible for these counters to rollover during the service life of the device (see discussion in Section 3.1.6 of [RFC 2863]).

6.6 SNMPv3 Notification Receiver config file element

This section specifies processing requirements on the CM when one or SNMPv3 Notification Receiver TLVs are present in the configuration file. The SNMPv3 Notification Receiver TLV is used to configure SNMPv3 tables for notification transmission. The CM MUST process this TLV only if the CM is in SNMPv3 Coexistence Mode.

Based on the TLV, the CM MUST make entries to the following tables in order to cause the desired trap transmission: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable, and vacmViewTreeFamilyTable. The mapping from the TLV to these tables is described in the following section.

6.6.1 Mapping of TLV fields into created SNMPv3 table rows

The following tables illustrate how the fields from the config file TLV elements are placed into the SNMPv3 tables. The TLV fields are shown below as:

<IP Address>

A 32-bit IP address of a notification receiver

<Port>

A 16-bit UDP Port number on the notification receiver to receive the notifications

<Trap type>

Defines the notification type as explained above

<Timeout>

16-bit timeout, in milliseconds to wait before sending a retry of an Inform Notification

<Retries>

16-bit number of times to retry an Inform after the first Inform transmission

<Filter OID>

The OID of the snmpTrapOID value that is the root of the MIB subtree that defines all of the notifications to be sent to the Notification Receiver

<Security Name>

The security name specified on the TLV element, or “@config” if not specified

These tables are shown in the order that the agent will search down through them when a notification is generated in order to determine to whom to send the notification, and how to fill out the contents of the notification packet.

In configuring entries in these SNMPv3 tables, note the following:

- The Community Name for traps in SNMPv1 and SNMPv2 packets is configured as “public”. The Security Name in traps and informs in SNMPv3 packets where no security name has been specified is configured as “@Config”, in which case the security level is “noAuthNoPriv”.

- Several columnar objects are configured with a value beginning with the string “@config”. If these tables are configured through other mechanisms, Network operators should not use values beginning with “@config” to avoid conflicts with the mapping process specified here.

6.6.1.1 *snmpNotifyTable*

The snmpNotifyTable is defined in [RFC 3413], in the “Notification MIB Module” section.

Create 2 rows with fixed values if 1 or more TLV elements are present.

Table 6–5 - snmpNotifyTable

Column Name (* = Part of Index)	1st Row Column Value	2nd Row Column Value
* snmpNotifyName	“@config_inform”	“@config_trap”
snmpNotifyTag	“@config_inform”	“@config_trap”
snmpNotifyType	inform (2)	trap (1)
snmpNotifyStorageType	volatile (2)	volatile (2)
snmpNotifyRowStatus	Active (1)	active (1)

6.6.1.2 *snmpTargetAddrTable*

The snmpTargetAddrTable is defined in [RFC 3413], in the “Management Target MIB Module” section.

Create 1 row for each TLV element in the config file.

Table 6–6 - snmpTargetAddrTable

Column Name (* = Part of Index)	Column Value
* snmpTargetAddrName	“@config_n” Where n ranges from 0 to m-1 where m is the number of notification receiver TLV elements in the config file
snmpTargetAddrTDomain	snmpUDPDDomain = snmpDomains.1
snmpTargetAddrTAddress (IP Address and UDP Port of the Notification Receiver)	OCTET STRING (6)Octets 1-4: <IP Address>Octets 5-6: <Port>
snmpTargetAddrTimeout	<Timeout> from the TLV
snmpTargetAddrRetryCount	<Retries> from the TLV
snmpTargetAddrTagList	“@config_trap” if <Trap type> is 1, 2, or 4 “@config_inform” if <Trap type> is 3 or 5
snmpTargetAddrParams	“@config_n” (Same as snmpTargetAddrName value)
snmpTargetAddrStorageType	volatile (2)
snmpTargetAddrRowStatus	active (1)

6.6.1.3 *snmpTargetAddrExtTable*

The snmpTargetAddrExtTable is defined in [RFC 3413], in the “SNMP Community MIB Module” section.

Create 1 row for each TLV element in the config file.

Table 6-7 - *snmpTargetAddrExtTable*

Column Name (* = Part of Index)	Column Value
* snmpTargetAddrName	"@config_n" where n ranges from 0 to m-1, and m is the number of notification receiver TLV elements in the config file
snmpTargetAddrTMask	<zero-length octet string>
snmpTargetAddrMMS	0

6.6.1.4 *snmpTargetParamsTable*

The snmpTargetParamsTable is defined in [RFC 3413], in the "Management Target MIB Module" section.

Create 1 row for each TLV element in the config file. If <Trap type> is 1, 2, or 3, or if the <Security Name> Field is zero-length, create the table as follows:

Table 6-8 - *snmpTargetParamsTable for <Trap type> 1, 2, or 3*

Column Name (* = Part of Index)	Column Value
* snmpTargetParamsName	"@config_n" where n ranges from 0 to m-1, and m is the number of notification receiver TLV elements in the config file
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	SNMPv1 (0) if <Trap type> is 1 SNMPv2c (1) if <Trap type> is 2 or 3 SNMPv3 (3) if <Trap type> is 4 or 5
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	SNMPv1 (1) if <Trap type> is 1 SNMPv2c (2) If <Trap type> is 2 or 3 USM (3) if <Trap type> is 4 or 5 NOTE: The mapping of SNMP protocol types to value here are different from snmpTargetParamsMPModel
snmpTargetParamsSecurityName	"@config"
snmpTargetParamsSecurityLevel	noAuthNoPriv
snmpTargetParamsStorageType	volatile (2)
snmpTargetParamsRowStatus	active (1)

If <Trap type> is 4 or 5, and the <Security Name> Field is non-zero length, create the table as follows:

Table 6-9 - *snmpTargetParamsTable for <Trap type> 4 or 5*

Column Name (* = Part of Index)	Column Value
*snmpTargetParamsName	"@config_n" where n ranges from 0 to m-1, and m is the number of notification receiver TLV elements in the config file
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	SNMPv1 (0) if <Trap type> is 1 SNMPv2c (1) if <Trap type> is 2 or 3 SNMPv3 (3) if <Trap type> is 4 or 5
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	SNMPv1 (1) if <Trap type> is 1 SNMPv2c (2) if <Trap type> is 2 or 3 USM (3) if <Trap type> is 4 or 5 NOTE: The mapping of SNMP protocol types to value here are different from snmpTargetParamsMPModel
snmpTargetParamsSecurityName	<Security Name>
snmpTargetParamsSecurityLevel	The security level of <Security Name>
snmpTargetParamsStorageType	volatile (2)
snmpTargetParamsRowStatus	active (1)

6.6.1.5 *snmpNotifyFilterProfileTable*

The snmpNotifyFilterProfileTable is defined in [RFC 3413], in the “Notification MIB Module” section.

Create 1 row for each TLV that has a non-zero <Filter Length>.

Table 6–10 - snmpNotifyFilterProfileTable

Column Name (* = Part of Index)	Column Value
* snmpTargetParamsName	“@config_n” where n ranges from 0 to m-1, and m is the number of notification receiver TLV elements in the config file
snmpNotifyFilterProfileName	“@config_n” where n ranges from 0 to m-1, and m is the number of notification receiver TLV elements in the config file
snmpNotifyFilterProfileStorType	volatile (2)
snmpNotifyFilterProfileRowStatus	active (1)

6.6.1.6 *snmpNotifyFilterTable*

The snmpNotifyFilterTable is defined in [RFC 3413], in the “Notification MIB Module” section.

Create 1 row for each TLV that has a non-zero <Filter Length>.

Table 6–11 - snmpNotifyFilterTable

Column Name (* = Part of Index)	Column Value
* snmpNotifyFilterProfileName	“@config_n” where n ranges from 0 to m-1, and m is the number of notification receiver TLV elements in the config file
* snmpNotifyFilterSubtree	<Filter OID> from the TLV
snmpNotifyFilterMask	<zero-length octet string>
snmpNotifyFilterType	included (1)
snmpNotifyFilterStorageType	volatile (2)
snmpNotifyFilterRowStatus	active (1)

6.6.1.7 *snmpCommunityTable*

The snmpCommunityTable is defined in [RFC 3413], in the “SNMP Community MIB Module” section.

Create 1 row with fixed values if 1 or more TLVs are present. This causes SNMPv1 and v2c notifications to contain the community string in snmpCommunityName.

Table 6–12 - snmpCommunityTable

Column Name (* = Part of Index)	Column Value
* snmpCommunityIndex	“@config”
snmpCommunityName	“public”
snmpCommunitySecurityName	“@config”
snmpCommunityContextEngineID	<the engineID of the cable modem>
snmpCommunityContextName	<zero-length octet string>
snmpCommunityTransportTag	<zero-length octet string>
snmpCommunityStorageType	volatile (2)
snmpCommunityStatus	active (1)

6.6.1.8 usmUserTable

The usmUserTable is defined in [RFC 3414], in the “Definitions” section.

Create 1 row with fixed values if 1 or more TLVs are present. Other rows are created, one each time the engine ID of a trap receiver is discovered. This specifies the user name on the remote notification receivers to which notifications are to be sent.

One row in the usmUserTable is created. When the engine ID of each notification receiver is discovered, the agent copies this row into a new row and replaces the 0x00 in the usmUserEngineID column with the newly-discovered value.

Table 6–13 - usmUserTable

Column Name (* = Part of Index)	Column Value
* usmUserEngineID	0x00
* usmUserName	“@config” When other rows are created, this is replaced with the <Security Name> field from the TLV element.
usmUserSecurityName	“@config” When other rows are created, this is replaced with the <Security Name> field from the TLV element.
usmUserCloneFrom	<don’t care> This row cannot be cloned.
usmUserAuthProtocol	None When other rows are created, this is replaced with None or MD5, depending on the security level of the V3 User.
usmUserAuthKeyChange	<don’t care> Write-only
usmUserOwnAuthKeyChange	<don’t care> Write-only
usmUserPrivProtocol	None When other rows are created, this is replaced with None or DES, depending on the security level of the V3 User.
usmUserPrivKeyChange	<don’t care> Write-only
usmUserOwnPrivKeyChange	<don’t care> Write-only
usmUserPublic	<zero-length string>
usmUserStorageType	volatile (2)
usmUserStatus	active (1)