



***Society of Cable
Telecommunications
Engineers***

**ENGINEERING COMMITTEE
Data Standards Subcommittee**

AMERICAN NATIONAL STANDARD

ANSI/SCTE 22-3 2012

**Data-Over-Cable Service Interface Specification
DOCSIS 1.0 Operations Support System Interface (OSSI)**

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. 2012

140 Philips Road

Exton, PA 19341

Contents

1	INTRODUCTION.....	1
1.1	Requirements	1
2	CM AND CMTS MANAGEMENT REQUIREMENTS.....	1
2.1	Accounting Management	1
2.2	Configuration Management.....	2
2.2.1	Version Control	2
2.2.2	Software upgrades	2
2.2.3	System Initialization and Configuration	2
2.3	Fault Management.....	3
2.3.1	SNMP Usage.....	3
2.3.2	Event Logging.....	3
2.3.3	Trap and Syslog Throttling.....	3
2.3.4	Non-SNMP Fault Management protocols	4
2.4	Performance Management.....	4
2.5	Protocol Filters.....	5
2.6	Common Spectrum Management	5
2.7	Protocol.....	5
3	AREAS FOR FUTURE CONSIDERATION.....	5
4	MANAGEMENT INFORMATION BASE (MIB).....	6
4.1	MIB Organization.....	6
4.2	Managed Objects from Existing Standards	7
4.2.1	Requirements for RFC-1907.....	7
4.2.2	Requirements for RFC-2233.....	8
4.2.3	Requirements for RFC-2011.....	9
4.2.4	Requirements for RFC-1493.....	9
4.2.5	Requirements for RFC-2665.....	9
4.2.6	Requirements for RFC-2013.....	9
4.2.7	Requirements for RFC-1512.....	9
4.3	MIB Transition	9
	APPENDIX I PROTOCOL DEFINITION FOR SYSLOG (NORMATIVE).....	10
	APPENDIX II REFERENCES (INFORMATIVE)	11
	APPENDIX III GLOSSARY (INFORMATIVE)	13
	APPENDIX IV MIB REQUIREMENTS (NORMATIVE).....	17
	APPENDIX V USB MIB DEFINITION (NORMATIVE)	19

List of Figures

Figure 4-1. Interface Numbering Example	8
---	---

This page intentionally left blank.

1 INTRODUCTION

This document outlines the Management Information Bases (MIBs) for high-speed data-over-cable systems developed by the DOCSIS Data Over Cable Services working group.

Three Simple Network Management Protocol (SNMP) MIBs are defined. The first is the DOCSIS Radio Frequency Interface (RFI) MIB and defines objects that enable management of the CATV MAC and PHY layer interfaces. The second is the DOCSIS Cable Device (CD) MIB and defines objects that enable management of CMs and Cable Modem Termination Systems (CMTSs). The third is DOCSIS Base Line Interface (BPI) MIB and defines objects that enable management of security features in the CM and CMTS.

This specification is intended to enable prospective vendors of cable modems and other data-over-cable systems to address the operations support requirements in a uniform and consistent manner.

1.1 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.

2 CM AND CMTS MANAGEMENT REQUIREMENTS

This section describes the CM and CMTS management requirements. The MIBs compliant with these requirements are described in Section 4 and formally defined in Section 5.

2.1 Accounting Management

Although many different types of billing scenarios exist for operators, the only scenarios which require use of CM and CMTS managed objects are those based on metered usage or reserved bandwidth. Common practice by several Internet Service Providers (ISPs) allows usage-based billing based on peak rates. A DOCSIS provider can implement usage-based billing two ways: by polling the CMs, or by polling the CMTS.

In the first method, a service provider can poll the ifInOctets and ifOutOctets counters from the MIB-II [RFC-1213] Interfaces group on each CM. This has the advantage of enabling both upstream and downstream traffic metering with the potential disadvantage of affecting network performance.

The second metered billing method involves monitoring the docsIfCmtsServiceTotalDataSlots counter from the docsIfCmtsServiceTable on each CMTS. This has the advantage of avoiding congestion on the RF network; however, it enables upstream traffic metering only. In a typical ISP environment, a BSS polls the appropriate

counters on each customer device once every 15 minutes throughout a monthly billing cycle. This data is converted into an average utilization rate for the sample period. Doing so permits the ISP to bill based on peak bandwidth by choosing the sample ranked at the 90-95th percentile. Note that the billing system may also include time-of-day rate variations. The billing of reserved upstream MAC bandwidth is aided by information available from the docsIfQosProfileTable for each CM. These MIB variables report the upstream QoS characteristics, not just the nominal bandwidth, associated with each service ID and enable the service provider to bill for Grade of Service by verifying QoS.

2.2 Configuration Management

2.2.1 Version Control

The CM and CMTS SHOULD support software revision and operational parameter configuration interrogation. In particular, the fields of the sysObjectID Object Identifier (OID) of the CM should successively encode the vendor ID, the hardware platform, the hardware revision, the software/PROM major revision number, the software/PROM minor revision number, and (optionally) the software patch level. Each parameter MUST occupy exactly one field. The fields of the sysObjectID OID of the CMTS SHOULD use the same encoding.

Additionally, the CM MUST (and the CMTS SHOULD) include the same revision information in the vendor defined text of the sysDescr object in the MIB-II System Group [RFC-1213].

2.2.2 Software upgrades

The CM software upgrade process is documented in [DOCSIS7].

The mechanism to upgrade software from an SNMP manager MUST be supported by CMs, and SHOULD be supported by CMTSs. From a network management station, the operator:

- sets docsDevSwServer to the address of the TFTP server for software upgrades
- sets docsDevSwFilename to the file pathname of the software upgrade image
- sets docsDevSwAdminStatus to upgrade-from-mgt

docsDevSwAdminStatus MUST persist across resets/reboots until overwritten from an SNMP manager or via the CM configuration file.

The default state of docsDevSwAdminStatus MUST be allowProvisioningUpgrade(2) until it is overwritten by ignoreProvisioningUpgrade(3) following a successful SNMP-initiated software upgrade.

docsDevSwOperStatus MUST persist across resets to report the outcome of the last software upgrade attempt.

Both docsDevSwServer and docsDevSwFilename MUST behave according to their textual descriptions in the cable device MIB.

If a CM suffers loss of power or resets during an SNMP-initiated upgrade, the CM MUST resume the interrupted upgrade without requiring manual intervention.

One reason for the SNMP-initiated upgrade is to allow loading of a temporary software image (e.g., special diagnostic software) that differs from the software normally used on that modem without changing the provisioning database.

Note that software upgrades MUST NOT be accepted blindly by the cable modem. The processes defined in [DOCSIS7] for CM response following software upgrade failure MUST be supported.

2.2.3 System Initialization and Configuration

Most system configuration of CMs is performed through a combination of CATV MAC, DHCP, and TFTP exchanges. These exchanges are defined in detail in the Radio Frequency Interfaces Specification [DOCSIS7]. In particular, to enable event logging through SYSLOG, the DHCP server sets the log server option [RFC-2132] to the address of the SYSLOG server.

2.3 Fault Management

2.3.1 SNMP Usage

In the DOCSIS environment, the goals of fault management are the remote detection, diagnosis, and correction of network problems. Therefore, the CM MUST support SNMP management traffic across both the Ethernet and CATV MAC interfaces. Access may be restricted to support policy goals (see the docsDevNmAccessTable).

CM installation personnel can use SNMP queries from a station on the Ethernet to perform on-site CM and CATV MAC diagnostics and fault classification (note that this may require temporary provisioning of the CM from an Ethernet DHCP server). Further, future customer applications using SNMP queries can diagnose simple post-installation problems, avoiding visits from service personnel and minimizing help desk telephone queries.

Standard MIB-II support MUST be implemented to instrument interface status, packet corruption, protocol errors, etc. The transmission MIB for Ethernet-like objects [RFC-1643] MUST be implemented on each CM and CMTS Ethernet and Fast Ethernet port. The ifXTable [RFC-2233] SHOULD be implemented to provide discrimination between broadcast and multicast traffic.

The CM and CMTS MUST support managed objects for fault management of the PHY and MAC layers. The MIB includes variables to track PHY state such as codeword collisions and corruption, signal-to-noise ratios, transmit and receive power levels, propagation delays, micro-reflections, in channel response, and Sync loss. The MIB also includes variables to track MAC state such as collisions and excessive retries for requests, immediate data transmits, and initial ranging requests.

For fault management at all layers, the CM/CMTS MUST generate replies to SNMP queries (subject to policy filters) for counters and status, MUST send SNMP traps to one or more trap NMSs (subject to policy), and MUST send event logging to a SYSLOG server (if a log server is defined). The ifTestTable [RFC-2233] SHOULD be implemented for any diagnostic test procedures that can be remotely initiated.

2.3.2 Event Logging

Event logging and history provide vendors an opportunity for product differentiation. The ability to report useful logs may depend on semi-graceful failure modes and on the ability to record such in nonvolatile storage.

Events SHOULD be reported via log entries in a MIB, the SYSLOG facility (as documented in Appendix B), and SNMP traps. Reporting of events SHOULD be fully configurable by priority class. At minimum, it MUST be possible to disable SNMP Trap and SYSLOG transmission.

A local event log that is available via SNMP queries SHOULD be implemented to track events that cannot be reported at the time that they occur. This log SHOULD support a minimum of ten event log entries, and SHOULD persist across device reboots.

The definition and coding of events is vendor-specific. However, the standard set of error codes and messages listed in Appendix I of [DOCSIS 7] SHOULD be used to textually describe events where applicable.

In deference to the network operator who must troubleshoot multi-vendor networks, the circumstances and meaning of each event are reported as human-readable text. Vendors SHOULD provide time-of-day clocks in CMs to provide useful timestamping of events. Similarly, event logs SHOULD be persistent across device reboots. The depth of the event log is vendor-dependent, with oldest entries discarded as needed.

For each vendor-specific event that is reportable via TRAP, the vendor must create an enterprise-specific trap definition. Trap definitions MUST include docsDevEvText and SHOULD be defined according to section 3.2.2. of draft-ietf-ipcdn-cable-device-mib.txt.

The event framework described in this section MUST be implemented in CMs and SHOULD be implemented in CMTSs.

2.3.3 Trap and Syslog Throttling

The CM and CMTS MUST provide support for trap and syslog message throttling as described below. The network operator can employ message rate throttling or trap limiting by manipulating the appropriate MIB variables.

2.3.3.1 Rate Throttling

Network operators may employ either of two rate control methods. In the first method, the device ceases to send traps and SYSLOG messages when the rate exceeds the specified maximum message rate. It resumes sending traps only if reactivated by a network management station request.

In the second method, the device resumes sending traps when the rate falls below the specified maximum message rate. The network operator configures the specified maximum message rate by setting the measurement interval (in seconds), and the maximum number of trap and SYSLOG messages (excluding duplicates) to be transmitted within the measurement interval. The operator can query the operational throttling state (to determine whether traps are enabled or blocked by throttling) of the device, as well as query and set the administrative throttling state (to manage the rate control method) of the device.

2.3.3.2 Trap Limiting

Network operators may wish to limit the number of traps sent by a device over a specified time period. The device ceases to send traps and SYSLOG messages when the number of traps exceeds the specified threshold. It resumes sending traps only when the measurement interval has passed.

The network operator defines the maximum number of traps he is willing to handle and sets the measurement interval to a large number (in hundredths of a second). For this case, the administrative throttling state is set to stop at threshold which is the maximum number of traps.

See “Techniques for Managing Asynchronously Generated Alerts” [RFC-1224] for further information.

2.3.4 Non-SNMP Fault Management protocols

The OSS can use a variety of tools and techniques to examine faults at multiple layers. For the IP layer, useful non-SNMP based tools include ping (ICMP Echo and Echo Reply), traceroute (UDP and various ICMP Destination Unreachable flavors). Pings to a CM from its Ethernet side **MUST** be supported to enable local connectivity testing from a customer’s PC to the modem. The CM and CMTS **MUST** support IP end-station generation of ICMP error messages and processing of all ICMP messages.

2.4 Performance Management

At the CATV MAC layer, performance management focuses on the monitoring of the effectiveness of cable plant segmentation and rates of upstream traffic and collisions. Instrumentation is provided in the form of the standard interfaces statistics, as well as the docsifCmtsServiceTable and docsifCmServiceTable.

It is not anticipated that the CMTS upstream bandwidth allocation function will require active network management intervention and tuning. Nevertheless, management objects are provided in case tuning or direct control is necessary. The three key upstream contention intervals are the request interval, the immediate data interval, and the initial ranging maintenance interval. If the upstream collision rate of requests and immediate data is high relative to the upstream traffic bandwidth, then the network management system (NMS) might increase the size of the request and immediate data intervals, respectively. The NMS might increase the size of the initial ranging maintenance interval when the upstream collision rate of initial ranging messages is relatively high, such as at the conclusion of a wide-spread regional power outage. The NMS might also decrease the size of these contention intervals under low collision rate conditions, since these intervals occupy bandwidth that may be otherwise used for upstream transmission bandwidth. As a last resort, the NMS might change the guaranteed upstream bandwidth for one or more service IDs, to relieve upstream traffic congestion for key subscribers. The CM **MUST** implement MIB counters that report the number of contention interval collisions (measured as the number of contention interval retries) per service ID, and the CMTS **MUST** implement read-write MIB objects that control the size of the contention intervals for each upstream channel. The CMTS **SHOULD** implement a read-write MIB object that controls the guaranteed upstream bandwidth for each service ID.

At the LLC layer, the performance management focus is on bridge traffic management. The CM and CMTS (if the CMTS implements transparent bridging) **MUST** implement the Bridge MIB [RFC-1493], including the dot1dBase and dot1dTp groups. The CM and CMTS **MUST** implement a managed object that controls whether the 802.1d spanning tree protocol (STP) is run and topology update messages are generated; STP is unnecessary in hierarchical, loop-free topologies. If the STP is enabled for the CM/CMTS, then the CM/CMTS **MUST** implement the dot1dStp

group. These MIB groups' objects allow the NMS to detect when bridge forwarding tables are full, and enable the NMS to modify aging timers.

A final performance concern is the ability to diagnose unidirectional loss. Both the CM and CMTS MUST implement the MIB-II [RFC-1213] Interfaces group. When there exists more than one upstream or downstream channel, the CM/CMTS MUST implement an instance of IfEntry for each channel. The ifStack MIB [RFC-2233] MUST be used to define the relationships among the CATV MAC interfaces and their channels.

2.5 Protocol Filters

The CM MUST implement LLC and IP protocol filters. The LLC protocol filter entries can be used to limit CM forwarding to a restricted set of network-layer protocols (such as IP, IPX, NetBIOS, and Appletalk). The IP protocol filter entries can be used to restrict upstream or downstream traffic based on source and destination IP addresses, transport-layer protocols (such as TCP, UDP, and ICMP), and source and destination TCP/UDP port numbers. The CM MUST support a minimum of ten LLC protocol filter entries, and ten IP protocol filter entries.

2.6 Common Spectrum Management

The CMTS SHOULD implement the HFC RF Spectrum Management MIB [CSMI-MIB]. The definition of this MIB is likely to evolve, and vendors should anticipate changes in this area.

2.7 Protocol

The SNMPv1 protocol [RFC-1157] and the SNMPv2 protocol have been selected as the protocol for management of data-over-cable services and MUST be implemented. Many of the managed objects described in the MIB addendums are configurable parameters and allow read-write access. As operators of public data networks, most cable operators will wish to restrict access to those objects, both at the CM and CMTS. Two mechanisms are provided to accomplish this.

First, the docsDevNMAccessTable in the Cabel Device MIB described in [RFC-2670] provides a means of restricting access to particular network management stations over particular interfaces using specific community strings. For example, the CMTS may be configured to respond only to SNMP requests originating on its network-side interface.

Second, writable-access for individual managed objects is controlled through the provisioned configuration file as described in [DOCSIS7]. That is, each read-write object can be redefined at provisioning time to be read-only.

3 AREAS FOR FUTURE CONSIDERATION

This section outlines some areas for future consideration within this specification.

- Enterprise-specific traps will be defined in the future as dictated by field experience.
- Multicast service provisioning within the cable modem will be clearly defined.
- To support the billing of reserved downstream MAC bandwidth, the CMTS should implement the evolving RSVP/Integrated Services MIB(s). Because of the variety of output queuing mechanisms, comments are solicited for the management mechanisms to support this.