

SCTE • ISBE[®]

S T A N D A R D S

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 165-06 2019

IPCablecom 1.5 Part 6: MIBS Framework

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE 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•ISBE members.

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

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

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

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2019
140 Philips Road
Exton, PA 19341

Note: DOCSIS® and PacketCable™ are registered trademarks of Cable Television Laboratories, Inc., and used in this document with permission.

Table of Contents

1	INTRODUCTION	5
1.1	PURPOSE	5
1.2	REQUIREMENTS AND CONVENTIONS	6
2	REFERENCES	7
2.1	NORMATIVE REFERENCES	7
2.2	INFORMATIVE REFERENCES	7
3	TERMS AND DEFINITIONS	9
4	ABBREVIATIONS AND ACRONYMS	13
5	OVERVIEW.....	20
5.1	IPCABLECOM REFERENCE ARCHITECTURE	20
5.2	GENERAL REQUIREMENTS.....	20
5.2.1	<i>Provisioning and Network Management Service Provider</i>	<i>21</i>
5.2.2	<i>Support for Embedded MTAs.....</i>	<i>21</i>
5.2.3	<i>SNMP Considerations.....</i>	<i>22</i>
5.2.3.1	USM Requirements	23
5.2.3.2	VACM Requirements.....	23
5.3	FUNCTIONAL REQUIREMENTS.....	24
5.3.1	<i>IPCablecom Device Provisioning</i>	<i>24</i>
5.3.2	<i>Security</i>	<i>24</i>
5.3.3	<i>Voice Interfaces.....</i>	<i>24</i>
5.3.4	<i>IPCablecom Voice Call Signaling</i>	<i>25</i>
5.3.5	<i>Media Packet Transport.....</i>	<i>25</i>
5.3.6	<i>Fault Management</i>	<i>25</i>
5.3.7	<i>Performance Management.....</i>	<i>25</i>
5.3.8	<i>Event Management</i>	<i>25</i>
6	MIB MODULES AVAILABLE IN AN IPCABLECOM NETWORK	26
6.1	DOCSIS MIB MODULES	26
6.2	IF MIB	26
6.3	MIB II.....	26
6.3.1	<i>sysDescr Requirements</i>	<i>27</i>
6.3.2	<i>sysObjectID Requirements</i>	<i>27</i>
6.3.3	<i>"iftable" Requirements</i>	<i>27</i>
6.4	IPCABLECOM SIGNALING MIB	29
6.4.1	<i>MTA SIGNALING MIB General Configuration Information.....</i>	<i>29</i>
6.4.2	<i>MTA NCS MIB per Endpoint Data.....</i>	<i>29</i>
6.5	IPCABLECOM MTA MIB MODULE	29
6.6	EVENT MANAGEMENT MIB.....	29
6.7	SNMP MIB	30
6.8	IPCABLECOM EXTENSION MIB.....	30
6.8.1	<i>MTA MIB Extension:.....</i>	<i>30</i>
6.8.2	<i>Signaling MIB Extension.....</i>	<i>30</i>
6.9	EDOCSIS ESAFE MIB	30
6.10	BATTERY BACKUP UPS MIB	30
7	IPCABLECOM MIB MODULE IMPLEMENTATION.....	31

7.1	MTA COMPONENTS	31
7.2	MIB LAYERING.....	31

List of Figures

FIGURE 1. IPCABLECOM REFERENCE ARCHITECTURE.....	20
FIGURE 2. PARTITIONING OF MANAGEMENT DOMAINS.....	21
FIGURE 3. EMBEDDED AND STANDALONE MTA IMPLEMENTATIONS.....	22
FIGURE 4. E-MTA COMPONENTS.....	31
FIGURE 5. MIB LAYERING MODEL	32

List of Tables

TABLE 1. FUNCTIONAL MIB AREAS	5
TABLE 2. MIB MODULES IMPLEMENTED BY THE EMTA COMPONENT OF THE E-MTA.....	26
TABLE 3. RFC 2863 IFTABLE, MIB-OBJECT DETAILS FOR E-MTA DEVICE INTERFACES.....	28
TABLE 4. RFC 2011 IPNetToMedia MIB-OBJECT DETAILS FOR E-MTA DEVICE INTERFACES.....	28
TABLE 5. IPNetToPhysicalTable MIB OBJECT DETAILS	29

1 INTRODUCTION

1.1 Purpose

This specification describes the framework in which IP-Cablecom 1.5 MIB (Management Information Base) modules are described. It provides information on the management requirements of IP-Cablecom-compliant devices and functions and how these requirements are supported in the MIB modules. It is intended to support and complement the actual MIB module documents, which are issued separately. There are currently two sets of the MIB modules that describe the Management Information Base for the IP-Cablecom Multimedia Terminal Adapters (MTAs) as per Table 1 below:

- IP-Cablecom MIBs ([11], [12], [13], [14], [33])
- IETF MIBs ([36], [37], [38]).

The IP-Cablecom 1.5 compliant MTAs **MUST** implement the IP-Cablecom MIBs. The IP-Cablecom 1.5 compliant MTAs **MAY** implement the IETF MIBs.

This document addresses some aspects of the voice communications capabilities of an IP-Cablecom network. The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined by appropriate legal and regulatory authorities. Nothing in this specification is addressed to, or intended to affect, those issues. In particular, while this document uses standard terms such as "call," "call signaling," "telephony," etc., it will be evident from this document that while a Packet-Cable network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers. These differences may be significant for legal/regulatory purposes.

Table 1. Functional MIB Areas

IP-Cablecom Specification	Phase	IP-Cablecom MIB Modules	IETF MIB Modules
NCS Protocol	1.5	Signaling MIB and Signaling Extension MIB	Signaling MIB
MTA Device Provisioning	1.5	MTA MIB and MTA Extension MIB	MTA MIB
Codec	1.5	Signaling MIB	Signaling MIB
Security	1.5	MTA MIB	MTA MIB
Management Event Mechanism	1.5	Management Event MIB	Management Event MIB

1.2 Requirements and Conventions

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

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

2 REFERENCES

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

2.1 Normative References

In order to claim compliance with this standard, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this standard. Intellectual property rights may be required to implement these references.

- [1] ANSI/SCTE 165-01 2019, IPCablecom 1.5 Part 1: Architecture Framework Technical Report.
- [2] ANSI/SCTE 165-05 2019, IPCablecom 1.5 Part 5: MTA Device Provisioning.
- [3] IETF STD0062, Simple Network Management Protocol Version 3 (SNMPv3), December 2002.
- [4] ANSI/SCTE 23-03 2017, DOCSIS 1.1 Part 3: Operations Support System Interface.
- [5] IETF RFC 791/STD0005, Internet Protocol, J. Postel, September 1981.
- [6] IETF RFC 2011, SNMPv2 Management Information Base for the Internet Protocol using SMIV2, K. McClohrrie, November 1996.
- [7] IETF RFC 2863, The Interfaces Group MIB, K. McClohrrie, F. Kastenholz, June 2000.
- [8] ANSI/SCTE 107 2017, DOCSIS 1.1 Part 3: Embedded Cable Modem Devices.
- [9] CableLabs Definition MIB Specification, <http://www.cablelabs.com/specification/cablelabs-definition-mib-specification/>, CL-SP-MIB-CLABDEF, Cable Television Laboratories, Inc.
- [10] ANSI/SCTE 79-02 2016, DOCSIS 2.0 Part 2: Operations Support System Interface.
- [11] ANSI/SCTE 165-07 2019, IPCablecom 1.5 Part 7: MTA MIB.
- [12] ANSI/SCTE 165-08 2019, IPCablecom 1.5 Part 8: Signaling MIB.
- [13] ANSI/SCTE 165-20 2019, IPCablecom 1.5 Part 20: MTA Extension MIB Specification.
- [14] ANSI/SCTE 165-21 2016, IPCablecom 1.5 Part 21: Signaling Extension MIB Specification.
- [15] IETF RFC 2013, SNMPv2 MIB for the User Datagram Protocol Using SMIV2.
- [16] IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).
- [17] CableLabs Battery Backup MIB Specification, <http://www.cablelabs.com/specification/cablelabs-battery-backup-mib-specification/>, CL-SP-MIB-BB, Cable Television Laboratories, Inc.

2.2 Informative References

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

- [18] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, CM-SP-CMCI-C01-081104, Cable Television Laboratories, Inc.
- [19] ANSI/SCTE 165-03 2016, IPCablecom 1.5 Part 3: Network-Based Call Signaling Protocol.
- [20] ANSI/SCTE 165-10 2009, IPCablecom 1.5 Part 10: Security.
- [21] ANSI/SCTE 165-04 2019, IPCablecom 1.5 Part 4: Dynamic Quality-of-Service.

- [22] IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework.
- [23] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP).
- [24] IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).
- [25] IETF RFC 3413/STD0062, Simple Network Management Protocol (SNMP) Applications.
- [26] IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
- [27] IETF RFC 3415/STD0062, View-based Access Control Model (VACM) for Simple Network Management Protocol (SNMP).
- [28] IETF RFC 2578/STD0058, Structure of Management Information Version 2 (SMIv2).
- [29] IETF RFC 1493, Definitions of Managed Objects for Bridges.
- [30] IETF RFC 3665, Definitions of Managed Objects for the Ethernet-like Interface Types, September 2003.
- [31] IETF RFC 2959, Real-Time Transport Protocol Management Information Base
- [32] ANSI/SCTE 165-02 2016, IPCablecom 1.5 Part 2: Audio/Video Codecs.
- [33] ANSI/SCTE 165-15 2019, IPCablecom 1.5 Part 15: Management Event MIB Specification.
- [34] ANSI/SCTE 135-04 2019, DOCSIS 3.0 Part 4: Operations Support System Interface.
- [35] IETF RFC 4293, Management Information Base for the Internet Protocol (IP), April 2006.
- [36] IETF RFC 4682, Multimedia Terminal Adapter (MTA) Management Information Base for PacketCable- and IPCablecom-Compliant Devices. December 2006.
- [37] IETF RFC 5098, Signaling MIB for PacketCable and IPCablecom Multimedia Terminal Adapters (MTAs). February 2008.
- [38] RFC 5428, Management Event Management Information Base (MIB) for PacketCable- and IPCablecom-Compliant Devices. April 2009.

3 TERMS AND DEFINITIONS

IPCablecom specifications use the following terms:

Access Control	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes, or other system resources on a network.
Active	A service flow is said to be "active" when it is permitted to forward data packets. A service flow must first be admitted before it is active.
Admitted	A service flow is said to be "admitted" when the CMTS has reserved resources (e.g., bandwidth) for it on the DOCSIS network.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access."
Asymmetric Key	An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct.
Audio Server	An Audio Server plays informational announcements in IPCablecom network. Media announcements are needed for communications that do not complete and to provide enhanced information services to the user. The component parts of Audio Server services are Media Players and Media Player Controllers.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity that claims to have given the information.
Authorization	The act of giving access to a service or device if one has permission to have the access.
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set which must contain both an encryption algorithm and a message authentication algorithm (e.g., a MAC or an HMAC). In general, it may also contain a key-management algorithm, which does not apply in the context of IPCablecom.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
Cleartext	The original (unencrypted) state of a message or data. Also called plaintext.
Confidentiality	A way to ensure that information is not disclosed to anyone other than the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
Cryptanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext.
Digital certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate.
Digital signature	A data value generated by a public-key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum.
Downstream	The direction from the headend toward the subscriber location.
Encipherment	A method used to translate plaintext into ciphertext.
Encryption	A method used to translate plaintext into ciphertext.

Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or Multipoint Conference Unit (MCU).
Errored Second	Any 1-second interval containing at least one bit error.
Event Message	A message capturing a single portion of a connection.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow") A unidirectional sequence of packets associated with a Service ID (SID) and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
Flow [IP Flow]	A unidirectional sequence of packets identified by OSI Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Gateway	Devices bridging between the IP/Cablecom IP Voice Communication world and the PSTN. Examples are the Media Gateway, which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signaling Gateway, which sends and receives circuit switched network signaling to the edge of the IP/Cablecom network.
H.323	An ITU-T recommendation for transmitting and controlling audio and video information. The H.323 recommendation requires the use of the ITU-T H.225 and ITU-T H.245 protocol for communication control between a "gateway" audio/video endpoint and a "gatekeeper" function.
Header	Protocol control information located at the beginning of a protocol data unit.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access Transport Area.
Jitter	Variability in the delay of a stream of incoming packets making up a flow such as a voice communication.
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.
Key Management	The process of distributing shared symmetric keys needed to run a security protocol.
Key Pair	An associated public and private key where the correspondence between the two are mathematically related, but it is computationally infeasible to derive the private key from the public key.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
Network Layer	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
Network Management	The functions related to the management of data across the network.