SCTE | STANDARDS

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 24-6 2016 (R2022)

IPCablecom 1.0 Part 6: Management Information Base (MIB) Framework

NOTICE

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

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

NOTE: The user's attention is called to the possibility that compliance with this document may require the use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. SCTE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

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

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.

Document Types and Tags

Document Type: Specification
Document Tags:

☐ Test or Measurement	☐ Checklist	☐ Facility
☒ Architecture or Framework	☐ Metric	☒ Access Network
☐ Procedure, Process or Method	☐ Cloud	☐ Customer Premises

Document Release History

Release	Date
SCTE 24-6 2001	*3/28/2001*
SCTE 24-6 2004	*7/23/2004*
SCTE 24-6 2006	*5/19/2006*
SCTE 24-6 2009	*6/5/2009*
SCTE 24-6 2016	*10/7/2016*

Note: This document is a reaffirmation of SCTE 24-6 2016. No substantive changes have been made to this document. Information components may have been updated such as the title page, NOTICE text, headers, and footers.

Table of Contents

List of Figures

List of Tables

1 INTRODUCTION

1.1 Purpose

This standard describes the framework in which IPCablecom MIB (Management Information Base) modules are described. It provides information on the management requirements of IPCablecom 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.

This document addresses some aspects of the voice communications capabilities of an IPCablecom 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

IPCablecom Specification	Phase	MIB
NCS Protocol	1.0	Signaling MIB
MTA Device Provisioning	1.0	MTA MIB
Codec	1.0	Signaling MIB
Security	1.0	MTA 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 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 event 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 REFERENCES (NORMATIVE)

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.

[1] ANSI/SCTE 24-01 2016, IPCablecom 1.0 Part 1: Architecture Framework for the Delivery of Time-Critical Services over Cable Television Networks Using Cable Modems.

[2] ANSI/SCTE 24-05 2016, IPCablecom 1.0 Part 5: Media Terminal Adapter (MTA) Device Provisioning Requirements for the Delivery of Real-Time Services over Cable Television Using Cable Modems.

[3] IETF STD 62, Simple Network Management Protocol Version 3 (SNMPv3), December 2002, D. Harrington, R. Presuhn, B. Wijnen, J. Case, D. Levi, P. Meyer, B. Stewart, U. Blumenthal, K. McCloghrie, http://www.ietf.org.

[4] IETF RFC 2669, Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems, http://www.ietf.org

[5] ANSI/SCTE 23-03 2010, DOCSIS 1.1 Part 3: Operations Support System Interface.

[6] IETF STD 5, Internet Protocol, J. Postel, September 1981, http://www.ietf.org.

[7] IETF RFC 2011, SNMPv2 Management Information Base for the Internet Protocol using SMIv2, K. McCloghrie, November 1996, http://www.ietf.org.

[8] IETF RFC 2863, The Interfaces Group MIB, K. McCloghrie, F. Kastenholz, June 2000, http://www.ietf.org.

[9] ANSI/SCTE 107 2007, Embedded Cable Modem Devices.

[10] CableLabs Definition MIB Specification, CL-SP-MIB-CLABDEF-I10-120809, August 09, 2012, Cable Television Laboratories, Inc., http://www.cablelabs.com/specification/cablelabs-definition-mib-specification/.

[11] ANSI/SCTE 79-02 2009, Data-Over-Cable Systems 2.0 Operations Support System Interface

[12] ANSI/SCTE 24-07 2016, IPCablecom 1.0 Part 7: Media Terminal Adapter (MTA) Management Information Base (MIB) Requirements

[13] ANSI/SCTE 24-08 2016, IPCablecom 1.0 Part 8: Network Call Signaling Management Information Base (MIB) Requirements.

[14] IETF RFC 2013, SNMPv2 MIB for the User Datagram Protocol Using SMIv2.

[15] IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).

3 TERMS AND DEFINITIONS

The following is a master list terms and definitions used by IPCablecom 1.0:

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 IPCablecom 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 IPCablecom 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.
Network Management OSS	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.
Nonce	A random value used only once that is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
Off-Net Call	A communication connecting an IPCablecom subscriber out to a user on the PSTN.
On-Net Call	A communication placed by one customer to another customer entirely on the IPCablecom Network.
One-way Hash	A hash function that has an insignificant number of collisions upon output.
Plaintext	The original (unencrypted) state of a message or data. Also called cleartext.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to anyone other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information, thereby eliminating the need for a host to support the service.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key, for encryption and decryption, also known as an asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.
Root Private Key	The private signing key of the highest-level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures generated with the corresponding root private key.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.

Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed using encryption.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and single source and destination UDP/TCP port.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.
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.
Transit Delays	The time difference between the instant at which the first bit of a Protocol Data Unit (PDU) crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.
Trunk	An analog or digital connection from a circuit switch that carries user media content and may carry voice signaling (M_F, R_2, etc.).
Tunnel Mode	An IPsec (ESP or AH) mode that is applied to an IP tunnel, where an outer IP packet header (of an intermediate destination) is added on top of the original, inner IP header. In this case, the ESP or AH transform treats the inner IP header as if it were part of the packet payload. When the packet reaches the intermediate destination, the tunnel terminates and both the outer IP packet header and the IPsec ESP or AH transform are taken out.
Upstream	The direction from the subscriber location toward the headend.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory

4 ABBREVIATIONS AND ACRONYMS

The following is a master list of abbreviations for IPCablecom 1.0:

AAA	Authentication, Authorization and Accounting.
AES	Advanced Encryption Standard. A block cipher, used to encrypt the media traffic in IPCablecom.
AF	Assured Forwarding. This is a DiffServ Per Hop Behavior.
AH	Authentication header. An IPsec security protocol that provides message integrity for complete IP packets, including the IP header.
AMA	Automated Message Accounting. A standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies).
ASD	Application-Specific Data. A field in some Kerberos key management messages that carries information specific to the security protocol for which the keys are being negotiated.
AT	Access Tandem.
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
BAF	Bellcore AMA Format, also known as AMA.
BCID	Billing Correlation ID.
BPI+	Baseline Privacy Plus Interface Specification. The security portion of the DOCSIS 1.1 standard that runs on the MAC layer.
CA	Certification Authority. A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CA	Call Agent. The part of the CMS that maintains the communication state, and controls the line side of the communication.
CBC	Cipher Block Chaining mode. An option in block ciphers that combine (XOR) the previous block of ciphertext with the current block of plaintext before encrypting that block of the message.
CBR	Constant Bit Rate.
CDR	Call Detail Record. A single CDR is generated at the end of each billable activity. A single billable activity may also generate multiple CDRs.
CIC	Circuit Identification Code. In ANSI SS7, a two-octet number that uniquely identifies a DSO circuit within the scope of a single SS7 Point Code.
CID	Circuit ID (Pronounced "kid"). This uniquely identifies an ISUP DS0 circuit on a Media Gateway. It is a combination of the circuit's SS7 gateway point code and Circuit Identification Code (CIC). The SS7 DPC is associated with the Signaling Gateway that has domain over the circuit in question.
CIF	Common Intermediate Format.
CIR	Committed Information Rate.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax.
CMS	Call Management Server. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology. This is one example of an Application Server.
CMTS	Cable Modem Termination System. The device at a cable headend which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.

CMSS	Call Management Server Signaling.
Codec	COder-DECoder.
COPS	Common Open Policy Service protocol. Defined in RFC2748.
CoS	Class of Service. The type 4 tuple of a DOCSIS configuration file.
CRCX	Create Connection.
CSR	Customer Service Representative.
DA	Directory Assistance.
DE	Default. This is a DiffServ Per Hop Behavior.
DES	Data Encryption Standard.
DF	Delivery Function.
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default. Network Provider DHCP Server.
DNS	Domain Name Service.
DOCSIS®	Data-Over-Cable Service Interface Specifications.
DPC	Destination Point Code. In ANSI SS7, a 3-octet number which uniquely identifies an SS7 Signaling Point, either an SSP, STP, or SCP.
DQoS	Dynamic Quality-of-Service. Assigned on the fly for each communication depending on the QoS requested.
DSA	Dynamic Service Add.
DSC	Dynamic Service Change.
DSCP	DiffServ Code Point. A field in every IP packet that identifies the DiffServ Per Hop Behavior. In IP version 4, the TOS byte is redefined to be the DSCP. In IP version 6, the Traffic Class octet is used as the DSCP.
DTMF	Dual-tone Multi Frequency (tones).
EF	Expedited Forwarding. A DiffServ Per Hop Behavior.
E-MTA	Embedded MTA. A single node that contains both an MTA and a cable modem.
EO	End Office.
ESP	IPsec Encapsulating Security Payload. Protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. ‘F’ stands for "Fully Associated."
FEID	Financial Entity ID.
FGD	Feature Group D signaling.
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 2821 for details.
GC	Gate Controller.
GTT	Global Title Translation.
HFC	Hybrid Fiber/Coaxial. An HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the headend and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.
HMAC	Hashed Message Authentication Code. A message authentication algorithm, based on either SHA-1 or MD5 hash and defined in IETF RFC 2104.
HTTP	Hypertext Transfer Protocol. Refer to IETF RFC 1945 and RFC 2068.
IANA	Internet Assigned Numbered Authority. See www.ietf.org for details.

IC	Inter-exchange Carrier.
IETF	Internet Engineering Task Force. A body responsible, among other things, for developing standards used on the Internet. See www.ietf.org for details.
IKE	Internet Key Exchange. A key-management mechanism used to negotiate and derive keys for SAs in IPsec.
IKE–	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
IKE+	A notation defined to refer to the use of IKE with X.509 certificates for authentication.
IP	Internet Protocol. An Internet network-layer protocol.
IPSec	Internet Protocol Security. A collection of Internet standards for protecting IP packets with encryption and authentication.
ISDN	Integrated Services Digital Network.
ISTP	Internet Signaling Transport Protocol.
ISUP	ISDN User Part. A protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ITU	International Telecommunication Union.
ITU-T	International Telecommunication Union–Telecommunication Standardization Sector.
IVR	Interactive Voice Response system.
KDC	Key Distribution Center.
LATA	Local Access and Transport Area.
LD	Long Distance.
LIDB	Line Information Database. Contains customer information required for real-time access such as calling card personal identification numbers (PINs) for real-time validation.
LLC	Logical Link Control. The Ethernet Packet header and optional 802.1P tag which may encapsulate an IP packet. A sublayer of the Data Link Layer.
LNP	Local Number Portability. Allows a customer to retain the same number when switching from one local service provider to another.
LSSGR	LATA Switching Systems Generic Requirements.
MAC	Message Authentication Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a MIC.
MAC	Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
MC	Multipoint Controller.
MCU	Multipoint Conferencing Unit.
MD5	Message Digest 5. A one-way hash algorithm that maps variable length plaintext into fixed-length (16 byte) ciphertext.
MDCP	Media Device Control Protocol. A media gateway control specification submitted to IETF by Lucent. Now called SCTP.
MDCX	Modify Connection.
MDU	Multi-Dwelling Unit. Multiple units within the same physical building. The term is usually associated with high-rise buildings.
MEGACO	Media Gateway Control IETF working group. See www.ietf.org for details.
MF	Multi-Frequency.
MG	Media Gateway. Provides the bearer circuit interfaces to the PSTN and transcodes the media stream.

MGC	Media Gateway Controller. The overall controller function of the PSTN gateway. Receives, controls and mediates call-signaling information between the IPCablecom and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF 2705.
MIB	Management Information Base.
MIC	Message Integrity Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a Message Authentication Code (MAC).
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSB	Most Significant Bit.
MSO	Multi-System Operator. A cable company that operates many headend locations in several cities.
MSU	Message Signal Unit.
MTA	Multimedia Terminal Adapter. Contains the interface to a physical voice device, a network interface, CODECs, and all signaling and encapsulation functions required for VoIP transport, class features signaling, and QoS signaling.
MTP	The Message Transfer Part. A set of two protocols (MTP 2, MTP 3) within the SS7 suite of protocols that are used to implement physical, data link, and network-level transport facilities within an SS7 network.
MWD	Maximum Waiting Delay.
NANP	North American Numbering Plan.
NANPNAT	North American Numbering Plan Network Address Translation.
NAT Network Layer	Network Address Translation. Layer 3 in the Open System Interconnection (OSI) architecture. This layer provides services to establish a path between open systems.
NCS	Network Call Signaling.
NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP).
NTP	Network Time Protocol. An internet standard used for synchronizing clocks of elements distributed on an IP network.
NTSC	National Television Standards Committee. Defines the analog color television broadcast standard used today in North America.
OID	Object Identification.
OSP	Operator Service Provider.
OSS	Operations Systems Support. The back-office software used for configuration, performance, fault, accounting, and security management.
OSS-D	OSS Default. Network Provider Provisioning Server.
PAL	Phase Alternate Line. The European color television format that evolved from the American NTSC standard.
PCES	IPCablecom Electronic Surveillance.
PCM	Pulse Code Modulation. A commonly employed algorithm to digitize an analog signal (such as a human voice) into a digital bit stream using simple analog-to-digital conversion techniques.
PDU	Protocol Data Unit.

PHS	Payload Header Suppression. A DOCSIS technique for compressing the Ethernet, IP, and UDP headers of RTP packets.
PKCROSS	Public-Key Cryptography for Cross-Realm Authentication. Utilizes PKINIT for establishing the inter-realm keys and associated inter-realm policies to be applied in issuing cross-realm service tickets between realms and domains in support of Intradomain and Interdomain CMS-to-CMS signaling (CMSS).
PKCS	Public-Key Cryptography Standards. Published by RSA Data Security Inc. These Standards describe how to use public key cryptography in a reliable, secure and interoperable way.
PKI	Public-Key Infrastructure. A process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
PKINIT	Public-Key Cryptography for Initial Authentication. The extension to the Kerberos protocol that provides a method for using public-key cryptography during initial authentication.
PSC	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
PSFR	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
PSTN	Public Switched Telephone Network.
QCIF	Quarter Common Intermediate Format.
QoS	Quality of Service. Guarantees network bandwidth and availability for applications.
RADIUS	Remote Authentication Dial-In User Service. An internet protocol (IETF RFC 2865 and RFC 2866) originally designed for allowing users dial-in access to the internet through remote servers. Its flexible design has allowed it to be extended well beyond its original intended use.
RAS	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
RC4	Rivest Cipher 4. A variable length stream cipher. Optionally used to encrypt the media traffic in IPCablecom.
RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html.
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Registered Jack-11. A standard 4-pin modular connector commonly used in the United States for connecting a phone unit into a wall jack.
RKS	Record Keeping Server. The device, which collects and correlates the various Event Messages.
RSA	A public-key, or asymmetric, cryptographic algorithm used to provide authentication and encryption services. RSA stands for the three inventors of the algorithm; Rivest, Shamir, Adleman.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
RTCP	Real-Time Control Protocol.
RTO	Retransmission Timeout.
RTP	Real-time Transport Protocol. A protocol for encapsulating encoded voice and video streams. Refer to IETF RFC 1889.
SA	Security Association. A one-way relationship between sender and receiver offering security services on the communication flow.

SAID	Security Association Identifier. Uniquely identifies SAs in the DOCSIS Baseline Privacy Plus Interface (BPI+) security protocol.
SCCP	Signaling Connection Control Part. A protocol within the SS7 suite of protocols that provides two functions in addition to those provided within MTP. The first function is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	Service Control Point. A Signaling Point within the SS7 network, identifiable by a Destination Point Code that provides database services to the network.
SCTP	Stream Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information delivered as a unit between peer service access points.
SF	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
SFID	Service Flow ID. A 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). Upstream Service Flow IDs and Downstream Service Flow IDs are allocated from the same SFID number space.
SFR	Service Flow Reference. A 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
SG	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular, the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1. A one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
SIP	Session Initiation Protocol. An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
SIP+	Session Initiation Protocol Plus. An extension to SIP.
S-MTA	Standalone MTA. A single node that contains an MTA and a non-DOCSIS MAC (e.g., ethernet).
SNMP	Simple Network Management Protocol.
SOHO	Small Office/Home Office.
SS7	Signaling System number 7. An architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Service Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
STP	Signal Transfer Point. A node within an SS7 network that routes signaling messages based on their destination address. This is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.
TCAP	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling Control Point.
TCP	Transmission Control Protocol.

TD	Timeout for Disconnect.
TFTP	Trivial File Transfer Protocol.
TFTP-D	Default – Trivial File Transfer Protocol.
TGS	Ticket Granting Server. A sub-system of the KDC used to grant Kerberos tickets.
TGW	Telephony Gateway.
TIPHON	Telecommunications and Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value. A tuple within a DOCSIS configuration file.
TN	Telephone Number.
ToD	Time-of-Day Server.
TOS	Type of Service. An 8-bit field of every IP version 4 packet. In a DiffServ domain, the TOS byte is treated as the DiffServ Code Point, or DSCP.
TSG	Trunk Subgroup.
UDP	User Datagram Protocol. A connectionless protocol built upon Internet Protocol (IP).
VAD	Voice Activity Detection.
VBR	Variable Bit Rate.
VoIP	Voice-over-IP.

5 OVERVIEW

IPCablecom MIB modules are designed to provide necessary functionality defined in IPCablecom specifications. The MIB design follows the same multi-phase schedule as the rest of IPCablecom specifications. MIB modules that are developed for IPCablecom 1.0 support Embedded-MTAs and in most cases Standalone MTAs, and provide definitions for call signaling and MTA device provisioning functions. Future IPCablecom development phases will include other functional areas as well as requirements for other IPCablecom components, which will be considered for MIB module development. Table 1 lists IPCablecom functional areas that are in the scope of IPCablecom 1.0.

5.1 IPCablecom Reference Architecture

The conceptual diagram for the IPCablecom architecture is shown in Figure 1. Please refer to the architecture document [1] for more detailed information concerning the IPCablecom architecture.

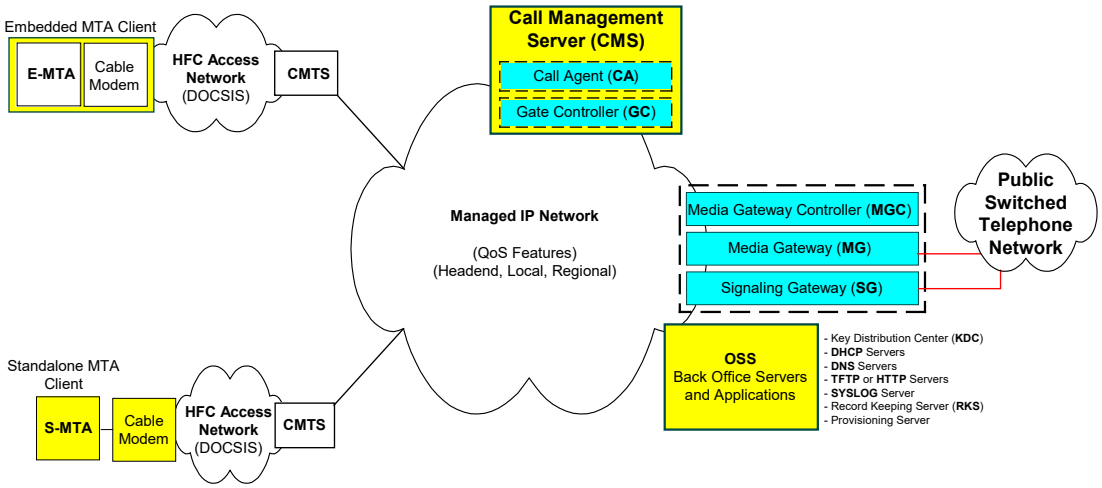

Figure 1. IPCablecom Reference Architecture

5.2 General Requirements

The IPCablecom MIBs Framework Specification follows the Internet Standard Management Framework described in RFC 3410 [19]. Additionally, the following requirements have been considered in the design of the IPCablecom MIB modules.

- IPCablecom 1.0 devices must be compliant with DOCSIS 1.1 or DOCSIS 2.0; therefore IPCablecom 1.0 devices MUST support DOCSIS 1.1 or DOCSIS 2.0 MIBs as defined in section 6.1 of this document.
- Take a minimalist approach for design of the IPCablecom MIB modules, i.e., if other MIB modules define the same functions, then rely on these MIB modules rather than create new ones.
- Organize MIB modules to support both Embedded and Standalone MTA. Note that IPCablecom 1.0 only requires Embedded MTA support.
- Organize MIB modules so as to allow functional partitioning of DOCSIS (high-speed data) and IPCablecom (voice) features.
- DOCSIS 1.1 or DOCSIS 2.0 within IPCablecom applications requires support of SNMPv3; therefore IPCablecom MIB agents MUST comply with SNMPv3.
- IPCablecom MIB modules MUST comply with SMIv2 as defined in IETF STD 58 [25].

In the following sections we will consider some of these requirements in detail.

5.2.1 Provisioning and Network Management Service Provider

A single physical device (e.g., embedded-MTA) will be completely provisioned and managed by a single business entity. In the case of multiple service providers offering different services on the same device (e.g., data by one provider, voice by another provider), a secondary service provider will act as the "contractor" for the primary provider in the areas of device provisioning and management.

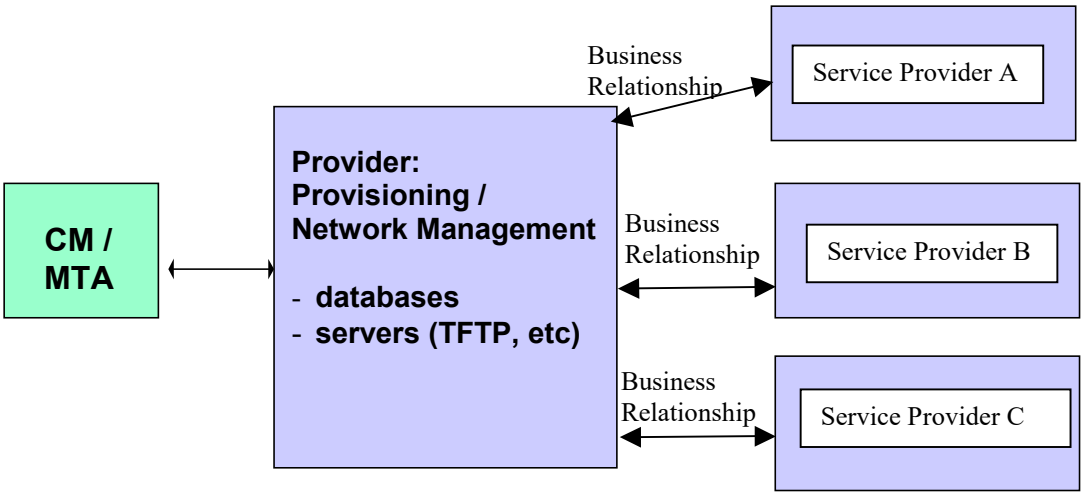

Figure 2. Partitioning of Management Domains

5.2.2 Support for Embedded and Standalone MTAs

The IPCablecom MIB modules include features for both Embedded and Standalone MTAs. Since the MTAs (Embedded or Standalone) are not required to support any DOCSIS related functions, they MUST NOT share any MIB objects in common with DOCSIS. The IPCablecom MIB modules are, however, designed to provide management support for voice related functions. DOCSIS Cable Modems with Embedded MTAs must adhere to the DOCSIS or eDOCSIS specifications related to the MIBs. The CM part of the-E-MTA MUST support eDOCSIS requirements defined in [7].

Figure 3 describes the possible MIB module implementation for an MTA (Embedded or Standalone):

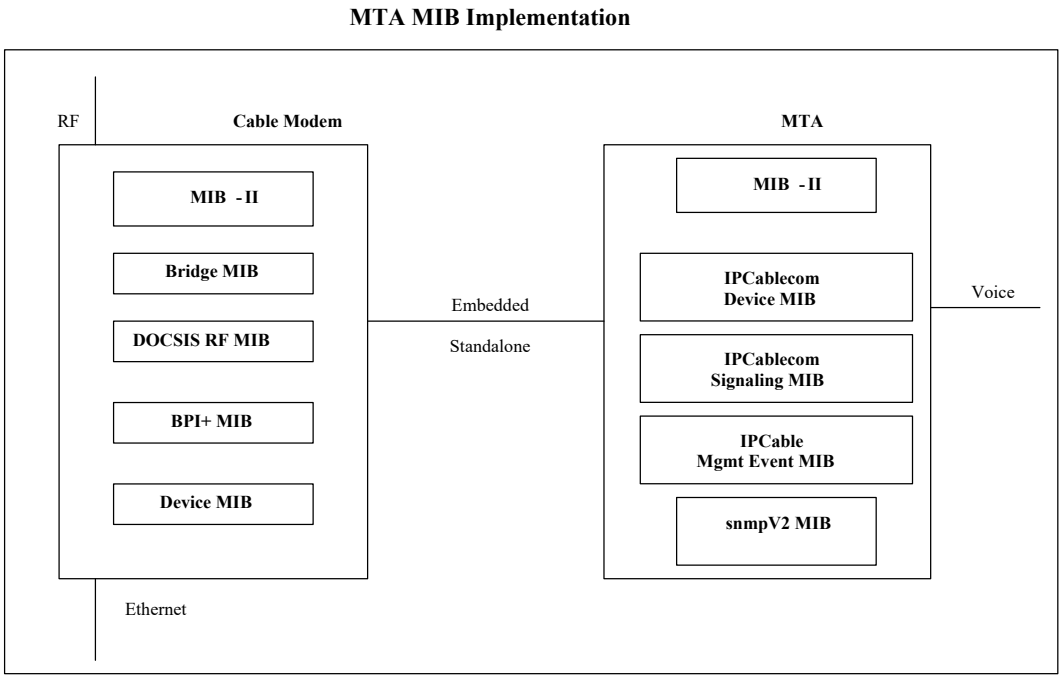

Figure 3. Embedded and Standalone MTA Implementations

5.2.3 SNMP Considerations

SNMPv3 provides an extended User Security Model, which implies changes to the way SNMP packets are exchanged between agents and managers. Since MIB modules are used to define the content of the packets, the changes for SNMPv3 do not affect MIB design.

IPCablecom MIB modules MUST conform to SMIv2 [25].

The following IETF RFCs provide more information on SNMPv3:

- IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework [19],
- IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) [20],
- IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) [21],
- IETF RFC 3413, Simple Network Management Protocol (SNMP) Applications [22],
- IETF RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) [23],
- IETF RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) [24].

5.2.3.1 USM Requirements

For IPCablecom 1.0, the usmUserTable MUST be configured immediately after the AP Reply received from the Provisioning Server with the following entries.

```
usmUserEngineID - the SNMP local engine id
usmUserName - MTA-Prov-xx:xx:xx:xx:xx:xx
usmUserSecurityName - MTA-Prov-xx:xx:xx:xx:xx:xx
usmUserCloneFrom – 0.0
usmUserAuthProtocol - usmHMACMD5AuthProtocol or
                      usmHMACSHAAuthProtocol
usmUserAuthKeyChange – ""
usmUserOwnAuthKeyChange – ""
usmUserPrivProtocol – usmDESPrivProtocol if privacy indicated in AP Reply,
usmNoPrivProtocol if no privacy is indicated in the AP Reply.
UsmUserPrivKeyChange – ""
UsmUserOwnPrivKeyChange – ""
usmUserPublic ‘’"
usmUserStorageType - permanent
usmUserStatus – active
```

The xx:xx:xx:xx:xx:xx in the usmUserName and usmUserSecurityName represents the MAC address of the MTA.

Initial authentication and privacy keys for this user are derived from the AP Reply message.

New users MAY be created by cloning as defined in SNMPv3. This MAY be done through the config file, or later through SNMP Set operations.

5.2.3.2 VACM Requirements

The following VACM entries MUST be defined for IPCablecom. Other table entries MAY be implemented at vendor or operator discretion.

VACM views MUST be defined for IPCablecom as described below.

5.2.3.2.1 VacmSecurityToGroup Table

The following configuration of the vacmSecurityToGroup table provides a read/write/create view.

```
vacmSecurityModel - USM
vacmSecurityName - "MTA-Prov-xx:xx:xx:xx:xx:xx’
vacmGroupName - 'PacketCableFullAccess'
vacmSecurityToGroupStorageType - permanent
vacmSecurityToGroupStatus - active
```

5.2.3.2.2 vacmAccessTable

The vacmAccessTable MUST be configured with the following entries. Other table entries MAY be implemented at vendor or operator discretion.

5.2.3.2.2.1 Full Access

This configuration allows for read access of all MIB modules in the MTA, write access to IPCablecom MIB modules, and notifications as defined in the IPCablecom MIB modules:

```
vacmGroupName – PacketCableFullAccess
vacmAccessContextPrefix – ""
vacmAccessSecurityModel - USM
vacmAccessSecurityLevel – authPriv or authNoPriv, depending on whether privacy has
been specified
vacmAccessContextMatch – exact
vacmAccessReadViewName – ReadOnlyView
vacmAccessWriteViewName – FullAccessView
vacmAccess NotifyViewName – NotifyView
vacmAccessStorageType – permanent
```

```
vacmAccessStatus - active
```

5.2.3.2.3 MIB View Requirements

The FullAccessView MUST consist of the MIB2 system group, the IFMIB, and all IPCablecom defined MIB modules. It MAY include vendor defined MIBs, VACM, USM, and Notifications MIB. The following lists the required OIDs:

```
1.3.6.1.2.1.1             /* MIB-II system group MIB tree */
1.3.6.1.2.1.2.2           /* MIB-II IF MIB tree */
1.3.6.1.4.1.4491.2.2      /* PacketCable Project MIB tree */
1.3.6.1.6.3.13            /* NOTIFY MIB tree */
1.3.6.1.6.3.15            /* USM MIB tree */
1.3.6.1.6.3.16            /* VACM MIB tree */
```

The ReadOnlyView MUST consist of the entire MIB tree contained in the MTA, including IPCablecom defined MIB modules, and vendor defined MIB modules for IPCablecom.

```
1.3.6.1                  /*  Full Internet MIB Tree*/
```

The NotifyView MUST consist of the MTA MIB tree, MIB-2 System MIB tree and the snmpTrapOID MIB. It MAY include vendor defined MIB modules.

```
1.3.6.1.4.1.4491.2.2.1  /* MTA mib tree*/
1.3.6.1.2.1.1           /* MIB-2 system mib tree */
1.3.6.1.6.3.1.1.4.1.0   /* snmpTrapOID mib*/
```

5.3 Functional Requirements

This section describes management functions that are supported by the IPCablecom MIB modules.

5.3.1 IPCablecom Device Provisioning

The IPCablecom 1.0 MIB modules should provide definitions for attributes that are required in the MTA device-provisioning flows. These attributes are documented in the IPCablecom MTA device provisioning specification [2] and include parameters such as CMS identifier, MTA domain name, MTA server addresses, and MTA capabilities. These attributes are defined as configuration file attributes and/or MIB objects as needed.

5.3.2 Security

The IPCablecom MIB modules provides definitions for attributes that are required for security handshake of the MTA and the provisioning server. These attributes include certificates and signatures.

5.3.3 Voice interfaces

IPCablecom MIB modules should provide a generic external interface to voice service management attributes. This should be done so as to allow a device to implement proprietary mechanisms for internal control and management of voice interfaces.

5.3.4 Packet Voice Call Signaling

The IPCablecom MIB modules should provide managed objects for the NCS call signaling protocol. Examples of attributes that have to be supported for packet voice call signaling include:

- Dial timeouts,
- Distinctive ring patterns,
- Codec capabilities,
- Signaling configuration for voice communication end points,
- Call agent identifier.

5.3.5 Media Packet Transport

The IPCablecom MIB modules do not provide any managed objects to monitor and manage media packet transport. The RTP and RTCP protocols are used for media transport in IPCablecom [29]. The RTP MIB (IETF RFC 2959 [28]) may be used for management of the media transport function of the MTA but this is considered out of scope for IPCablecom 1.0.

5.3.6 Fault Management

The IPCablecom MIB modules should provide objects for the management of network faults and failures. Some of these managed objects and management functions are defined in the IPCablecom MTA MIB [12] and the IPCablecom Signaling MIB [13] specifications. Further definition of default management is out of scope of IPCablecom 1.0.

5.3.7 Performance Management

The IPCablecom MIB modules should provide objects for the management of network performance when used for voice communications. Further definition of performance management is out of scope of IPCablecom 1.0.

6 MIB MODULES AVAILABLE IN AN IPCABLECOM NETWORK

In designing the IPCablecom MIBs Framework, the managed objects present in the other MIB modules implemented by the IPCablecom MTA device were taken into consideration. This section describes the MIB modules that can be present in the IPCablecom MTA, and may be used for IPCablecom management functions.

The following table lists the MIB modules that must be present in the IPCablecom MTAs. E-MTAs and S-MTAs MUST implement MIB modules present in Table 2.

Table 2. MIB Modules Implemented by E-MTA and S-MTA

IF MIB
MIB II
Ethernet MIB
Bridge MIB
IPCablecom 1.0 MTA Device MIB
IPCablecom 1.0 Signaling MIB
snmpV2 MIB group

As mentioned before, partitioning of voice and data services and support of both S-MTA and E-MTA has been part of the requirements for design of the IPCablecom MIBs Framework. Figure 3 in the General Requirements section describes possible organizations of the MIB modules in order to meet these requirements.

6.1 DOCSIS MIB Modules

As described in section 5.2, the IPCablecom 1.0 Embedded MTA must support the DOCSIS 1.1 or DOCSIS 2.0 MIB requirements. Refer to the following documents for the normative DOCSIS MIB requirements:

- For DOCSIS 1.1, the MIB module requirements are defined in section 3 of [5].
- For DOCSIS 2.0, the MIB module requirements are defined in section 6 of [11].

6.2 IF MIB

The Interfaces Group MIB (IF MIB) is defined in RFC 2863 [8]. The IF MIB is required for the definition of multiple interfaces in the MTA.

6.3 MIB II

RFC 3418 [15], RFC 2011 [7], and RFC 2013 [14] define the second version of the Management Information Base (MIB-II) for use with network management protocols in TCP/IP-based internet. Not all objects in this MIB are deemed necessary for the IPCablecom MTA device. The IPCablecom 1.0 MIB module only requires the system, interfaces, IP, and transmission objects of MIB II to be present in the MTA.

The system object group contact, administrative, location, and service information regarding the managed node.

6.3.1 sysDescr Requirements

The MTA's MIB II sysDescr object MUST conform to the format specified in DOCSIS OSSI [5].

6.3.2 sysObjectID Requirements

sysObjectID is defined as follows:

```
sysObjectID OBJECT-TYPE
SYNTAX  OBJECT IDENTIFIER
```

```
ACCESS  read-only
STATUS  mandatory
DESCRIPTION
   "The vendor's authoritative identification of the network
    management subsystem contained in the entity.  This
    value is allocated within the SMI enterprises subtree
    (1.3.6.1.4.1) and provides an easy and unambiguous
    means for determining `what kind of box' is being
    managed.  For example, if vendor `Flintstones, Inc.'
    was assigned the subtree 1.3.6.1.4.1.4242, it could
    assign the identifier 1.3.6.1.4.1.4242.1.1 to its `Fred
    Router'."
::= { system 2 }
```

By using sysObjectID the manager will be able to determine any enterprise specific MIBs which must be used to manage the embedded MTA.

6.3.3 "iftable" Requirements

IPCablecom ifTable MUST contain information about all IPCablecom endpoints. IfIndex, in case of IPCablecom MTAs MUST start with value of 9 for telephony endpoints and MUST be incremented sequentially and match the physical numbering of the telephony endpoints (Indices 2 through 8 are reserved for future use and the usage of index 1 is defined later in this section.) Each instance of the end-point in an E-MTA MUST have a corresponding entry ("conceptual row") in the "ifTable" MIB Table.

The cable modem part of an embedded MTA MUST adhere to DOCSIS 1.1 and eDOCSIS [9] requirements for MIB compliancy.

For each "conceptual row" in the "ifTable" table that corresponds to a Telephony Endpoint, the following conceptual columns MUST be used:

```
"ifIndex"
"ifDescr"
"ifType"
"ifAdminStatus"
"ifOperStatus"
```

Each conceptual row in "ifTable" MUST conform to the "IANAifType-MIB" definition for the IPCablecom interface type:

```
"ifType"    – voiceOverCable (198)
"ifDescr"   – "Voice Over Cable Interface"
```

IfIndex 1 is used to recognize the DOCSIS Cable Modem behind which an MTA is connected and the MIB modules involved are indicated in Tables 3 and 4. In the case of an embedded MTA the tables MUST be adhered to. For standalone MTAs, the MTA MAY choose to follow the same. In case a standalone MTA cannot display the information, ifIndex 1 MUST be left unused. If the standalone MTA is behind a CableHome or other device for its data connectivity it MAY change the ifDescr to reflect the same.

IPCablecom MTAs MUST implement [5], [6], and [7]. IPCablecom implementation MUST conform to the ifTable and ipNetToMediaTable defined below:

Table 3. RFC 2863 ifTable, MIB-Object Details for embedded MTA Device Interfaces

RFC-2863 MIB-Object Details for MTA Device Interface	MTA Device
IfIndex	1
ifDescr: MUST match the text provided in the next column.	"DOCSIS Embedded Interface "
IfType	other(1)
IfMtu	0

IfSpeed	0
ifPhysAddress	eMTA MAC address
IfAdminStatus : Only up control is required for this interface, down(2) and testing(3) is out of the scope of this specification.	up(1)
ifOperStatus: only up report is required for this object, other options are out of the scope of this specification.	up(1)
IfLastChange	per RFC 2863
ifInOctets: This object is optional, if not implemented, it MUST return 0	(n), 0
IfInNUCastPkts	Deprecated
IfInDiscards	0
IfInErrors	0
IfUnknownProtos	0
ifOutOctets: This object is optional, if not implement MUST return 0	(n), 0
ifOutUCastPkts: This object is optional, if not implemented, it MUST return 0	(n), 0
IfOutNUCastPkts	Deprecated
IfOutDiscards	0
IfOUtErrors	0
IfOutQlen	Deprecated
IfSpecific	Deprecated
ifXTable : entries in ifXtable for this type of interface are not required	NA

Table 4. RFC 2011 ipNetToMedia MIB-Object Details for eMTA Device Interfaces

RFC-2011 MIB-Object details for MTA Devices Interfaces	CM Device
IpNetToMediaIfIndex	1
IpNetToMediaPhysAddress	CM MAC Address
IpNetToMediaNetAddress	Acquired CM IP address
IpNetToMediaType	Static(4)
IfIndex	1

6.4 Ethernet MIB

The Ethernet MIB specifies the definitions of managed objects for the Ethernet-like interfaces (RFC 3665 [27]).

6.5 IPCablecom Signaling MIB

The IPCablecom Signaling MIB module is defined in [13]. It describes Call Signaling information for the MTA device provisioning and configuration. The IPCablecom Signaling MIB module is registered under the CableLabs private enterprise MIB under the IPCablecom Project branch `(clabProjPacketCable)`.

The IPCablecom Signaling MIB module contains general configuration information that applies to the Network Call Signaling (NCS) protocol [16] on a per MTA device basis. This data only provides the means to provision call signaling parameters on a device basis.

The IPCablecom Signaling MIB module also defines managed objects applicable on a per endpoint basis. The NCS endpoint table (pktcSigEndPntConfigTable) contains specific NCS endpoint configuration information. This data only provides the means to provision network call signaling per endpoint.

6.5.1 MTA SIGNALING MIB General Configuration Information

The MTA SIGNALING MIB contains general configuration information that applies to network call signaling on a device basis.

This data only provides the means to provision call signaling on a device basis.

6.5.2 MTA NCS MIB per Endpoint Data

The MTA NCS MIB contains a per endpoint table. This table contains general configuration information that applies to network call signaling on a per endpoint basis. This information is also found in the configuration file defined in the IPCablecom NCS specification [16]. This data only provides the means to provision network call signaling per endpoint.

6.6 IPCablecom MTA MIB Module

The IPCablecom MTA MIB module is defined in [12]. It describes data for provisioning the MTA device. The IPCablecom MTA MIB module is registered under the CableLabs private enterprise MIB under the IPCablecom Project branch `(clabProjPacketCable)`.

The IPCablecom MTA MIB module contains general configuration information to provision the MTA device. These objects describe the provisioning data for the required servers, the MTA security information.

7 IPCABLECOM MIB MODULE IMPLEMENTATION

This section describes a reference implementation of the MIB modules in an IPCablecom device. Given that only E-MTA is supported for the IPCablecom 1.0 release, we will only consider E-MTA type implementations in this section.

7.1 MTA Components

Figure 4 below shows the components of a typical MTA.

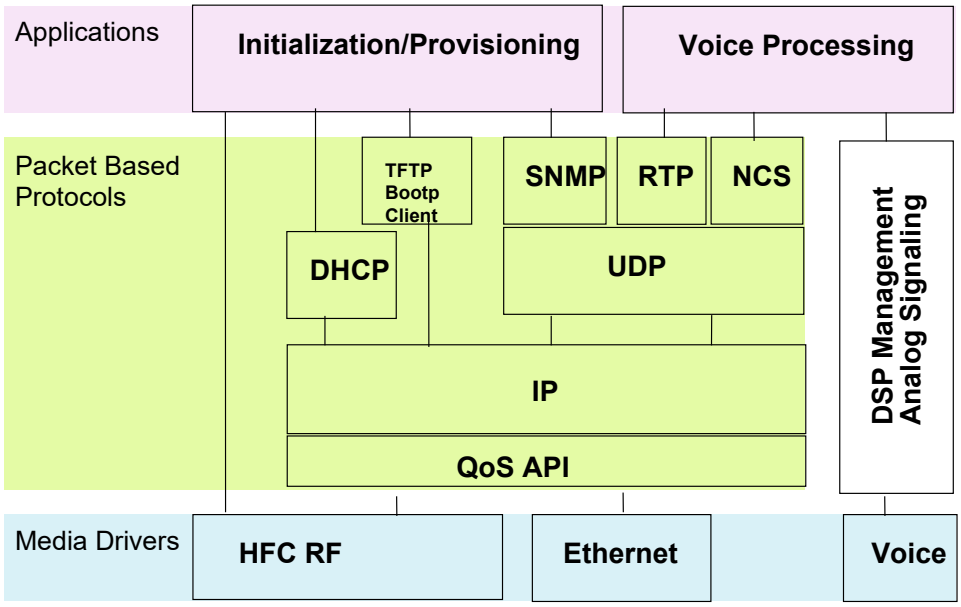

Figure 4. MTA Components

As shown here the MTA components can be organized into separate areas, i.e., packet based protocols, which run on top of IP and the voice subsystem, which consists of DSP engines and their associated software. MIB modules that are implemented in the MTA have to be organized so as to facilitate this separation. IPCablecom 1.0 MIB modules specifies functions for the packet based protocol section of the MTA. As of this writing there are no analog voice MIB modules specified for the MTA.

NOTE: Please refer to the IPCablecom Security Specification [17] for the security protocols.

7.2 MIB Layering

Figure 5 below describes the MIB layering model. The two stacks represent the packet network and analog voice sections of the MTA. On the packet network side MIB layering follows the same layering model as the protocol stacks.

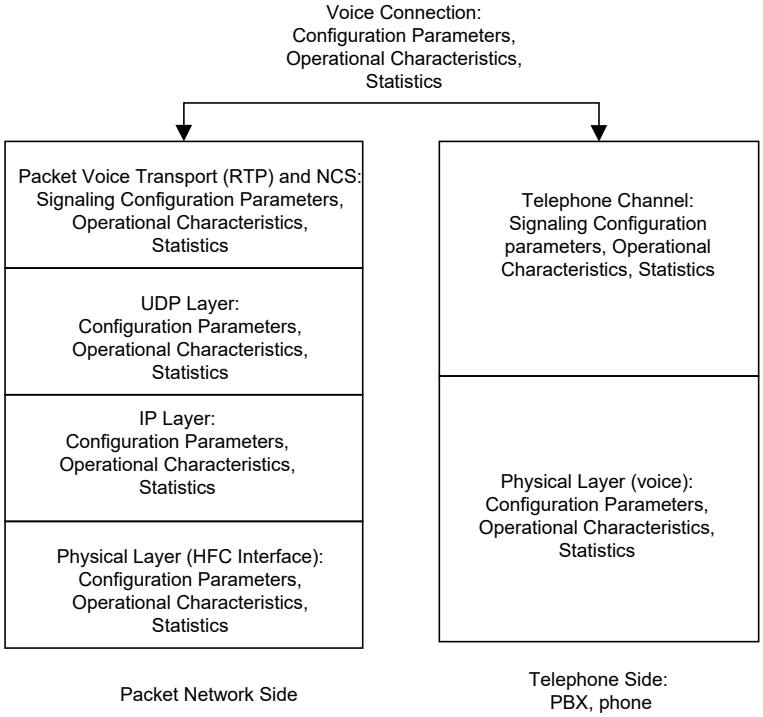

Figure 5. MIB Layering Model

In the context of voice communications, MIB modules can be layered into the physical layer attributes, which deal with the voice interface, and the telephone channel attributes which deal with voice signaling. Note that IPCablecom 1.0 does not specify any MIB modules for the telephone side of the MTA.

Appendix I Bibliography (Informative)

[16] ANSI/SCTE 24-03 2016, IPCablecom 1.0 Part 3: Network Call Signaling Protocol for the Delivery of Time-Critical Services over Cable Television Using Data Modems

[17] ANSI/SCTE 24-10 2016, IPCablecom 1.0 Part 10: Security Specification.

[18] ANSI/SCTE 24-04 2016, IPCablecom 1.0 Part 4: Dynamic Quality of Service for the Provision of Real-Time Services over Cable Television Networks Using Data Modem

[19] IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework.

[20] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP).

[21] IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).

[22] IETF RFC 3413, Simple Network Management Protocol (SNMP) Applications.

[23] IETF RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).

[24] IETF RFC 3415, View-based Access Control Model (VACM) for Simple Network Management Protocol (SNMP).

[25] IETF STD 58, Structure of Management Information Version 2 (SMIv2).

[26] IETF RFC 1493, Definitions of Managed Objects for Bridges.

[27] IETF RFC 3665, Definitions of Managed Objects for the Ethernet-like Interface Types, September 2003.

[28] IETF RFC 2959, Real-Time Transport Protocol Management Information Base

[29] ANSI/SCTE 24-02 2016, IPCablecom 1.0 Part 2: Audio Codec Requirements for the Provision of Bi-directional Audio Service Over Cable Television Networks Using Cable Modems