

# **Superseded** **by a later version of this document**

## **PacketCable™ 1.5 Specifications**

### **MIBs Framework Specification**

**PKT-SP-MIBS1.5-I01-050128**

**ISSUED**

#### **Notice**

This PacketCable specification is a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. (CableLabs®) for the benefit of the cable industry. Neither CableLabs, nor any other entity participating in the creation of this document, is responsible for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document by any party. This document is furnished on an AS-IS basis and neither CableLabs, nor other participating entity, provides any representation or warranty, express or implied, regarding its accuracy, completeness, or fitness for a particular purpose.

© Copyright 2004-2005 Cable Television Laboratories, Inc.  
All rights reserved.

## Document Status Sheet

<b>Document Control Number:</b>	PKT-SP-MIBS1.5-I01-050128		
<b>Document Title:</b>	MIBs Framework Specification		
<b>Revision History:</b>	D01 — Released September 30, 2004 I01 — Issued January 28, 2005		
<b>Date:</b>	Issued January 28, 2005		
<b>Status:</b>	<del>Work in Progress</del>	<del>Draft</del>	Issued
<b>Distribution Restrictions:</b>	<del>Author Only</del>	<del>CL/Member</del>	Public
		<del>CL/ PacketCable/ Vendor</del>	

### Key to Document Status Codes:

<b>Work in Progress</b>	An incomplete document designed to guide discussion and generate feedback, which may include several alternative requirements for consideration.
<b>Draft</b>	A document in specification format considered largely complete, but lacking reviews by Members and vendors. Drafts are susceptible to substantial change during the review process.
<b>Issued</b>	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
<b>Closed</b>	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

### Trademarks:

DOCSIS®, eDOCSIS™, PacketCable™, CableHome®, CableOffice™, OpenCable™, CableCARD™, and CableLabs® are trademarks of Cable Television Laboratories, Inc.

# Contents

<b>1 INTRODUCTION .....</b>	<b>1</b>
1.1 Purpose .....	1
1.2 Specification Language .....	2
<b>2 REFERENCES .....</b>	<b>3</b>
2.1 Normative .....	3
2.2 Informative .....	3
2.3 Reference Acquisition.....	4
<b>3 TERMS AND DEFINITIONS .....</b>	<b>5</b>
<b>4 ABBREVIATIONS .....</b>	<b>9</b>
<b>5 OVERVIEW .....</b>	<b>16</b>
5.1 PacketCable Reference Architecture .....	16
<b>5.2 General Requirements .....</b>	<b>16</b>
5.2.1 Provisioning and Network Management Service Provider .....	17
5.2.2 Support for Embedded MTAs .....	17
5.2.3 SNMP Considerations.....	18
<b>5.3 Functional Requirements .....</b>	<b>21</b>
5.3.1 PacketCable Device Provisioning.....	21
5.3.2 Security .....	21
5.3.3 Voice interfaces .....	21
5.3.4 PacketCable Voice Call Signaling .....	21
5.3.5 Media Packet Transport.....	21
5.3.6 Fault Management.....	21
5.3.7 Performance Management .....	21
5.3.8 Event Management.....	21
<b>6 MIB MODULES AVAILABLE IN A PACKETCABLE NETWORK .....</b>	<b>23</b>
6.1 DOCSIS MIB Modules.....	23
6.2 IF MIB .....	23
<b>6.3 MIB II .....</b>	<b>23</b>
6.3.1 sysDescr Requirements.....	23
6.3.2 sysObjectID Requirements .....	24
6.3.3 "iftable" Requirements .....	24
6.4 Ethernet MIB.....	26
6.5 PacketCable SIGNALING MIB.....	26

6.5.1 MTA SIGNALING MIB general configuration information.....	26
6.5.2 MTA NCS MIB per endpoint data .....	26
<b>6.6 PacketCable MTA MIB module .....</b>	<b>26</b>
<b>6.7 Event Management MIB .....</b>	<b>26</b>
<b>6.8 SNMP MIB .....</b>	<b>26</b>
<b>6.9 PacketCable Extension MIB .....</b>	<b>26</b>
6.9.1 MTA MIB Extension: .....	27
6.9.2 Signaling MIB Extension .....	27
6.9.3 Syslog MIB.....	27
<b>7 PACKETCABLE MIB MODULE IMPLEMENTATION.....</b>	<b>28</b>
<b>7.1 MTA components .....</b>	<b>28</b>
<b>7.2 MIB Layering .....</b>	<b>28</b>
<b>APPENDIX A. ACKNOWLEDGEMENTS.....</b>	<b>30</b>

## List of Figures

Figure 1. PacketCable Reference Architecture.....	16
Figure 2. Partitioning of Management Domains.....	17
Figure 3. Embedded and Standalone MTA implementations.....	18
Figure 4. E-MTA Components .....	28
Figure 5. MIB Layering Model .....	29

## List of Tables

Table 1. Functional MIB Areas.....	1
Table 2. MIB modules implemented by E-MTA.....	23
Table 3. RFC 2863 ifTable, MIB-Object Details for E-MTA Device Interfaces.....	25
Table 4. RFC 2011 ipNetToMedia MIB-Object Details for E-MTA Device Interfaces .....	25

by a later version of this document

## 1 INTRODUCTION

### 1.1 Purpose

This specification describes the framework in which PacketCable™ 1.5 MIB (Management Information Base) modules are described. It provides information on the management requirements of PacketCable 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 a PacketCable 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 PacketCable 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**

<b>PacketCable Specification</b>	<b>Phase</b>	<b>MIB</b>
NCS Protocol	1.5	Signaling MIB and Signaling Extension MIB
MTA Device Provisioning	1.5	MTA MIB and MTA Extension MIB
Codec	1.5	Signaling MIB
Security	1.5	MTA MIB
Management Event MIB	1.5	Management Event MIB

## 1.2 Specification Language

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 REFERENCES

### 2.1 Normative

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

- [1] PacketCable 1.5 Architecture Framework, PKT-TR-ARCH1.5-I01-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.
- [2] PacketCable 1.5 MTA Device Provisioning Specification, PKT-SP-PROV1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.
- [3] IETF STD0062, Simple Network Management Protocol Version 3 (SNMPv3), December 2002.
- [4] IETF RFC 2669, Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems.
- [5] Data-Over-Cable Service Interface Specifications, DOCSIS 1.1, Operations Support System Interface, SP-OSSIV1.1-I07-030730, July 30, 2003, Cable Television Laboratories, Inc.
- [6] IETF RFC 791/STD0005, Internet Protocol, J. Postel, September 1981.
- [7] IETF RFC 2011, SNMPv2 Management Information Base for the Internet Protocol using SMIV2, K. McCloghrie, November 1996.
- [8] IETF RFC 2863, The Interfaces Group MIB, K. McCloghrie, F. Kastenholz, June 2000.
- [9] Data-Over-Cable Service Interface Specifications, eDOCSIS™ Specification, CM-SP-eDOCSIS-I04-04041124, November 11, 2004, Cable Television Laboratories, Inc.
- [10] CableLabs Definition MIB Specification, CL-SP-MIB-CLABDEF-I04-040804, August 04, 2004, Cable Television Laboratories, Inc.
- [11] Data-Over-Cable Service Interface Specifications, DOCSIS 2.0, Operations Support System Interface Specification, SP-OSSIV2.0-I07-041210, December 10, 2004, Cable Television Laboratories, Inc.
- [12] PacketCable 1.5 MTA MIB Specification, PKT-SP-MIB-MTA1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.
- [13] PacketCable 1.5 Signaling MIB Specification, PKT-SP-MIB-SIG1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.
- [14] PacketCable 1.5 MTA Extension MIB Specification, PKT-SP-MIB-EXMTA1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.
- [15] PacketCable 1.5 Signaling Extension MIB Specification, PKT-SP-MIB-EXSIG1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.

### 2.2 Informative

- [16] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification (CMCI), SP-CMCI-I09-030730, July 30, 2003, Cable Television Laboratories, Inc.
- [17] PacketCable 1.5 Network-Based Call Signaling Protocol Specification, PKT-SP-NCS1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.

- [18] PacketCable 1.5 Security Specification, PKT-SP-SEC1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.
- [19] PacketCable Dynamic Quality of Service Specification, PKT-SP-DQOS1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.
- [20] IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework.
- [21] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP).
- [22] IETF RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP).
- [23] IETF RFC 3413/STD0062, Simple Network Management Protocol (SNMP) Applications.
- [24] IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3).
- [25] IETF RFC 3415/STD0062, View-based Access Control Model (VACM) for Simple Network Management Protocol (SNMP).
- [26] IETF RFC 2578/STD0058, Structure of Management Information Version 2 (SMIv2).
- [27] IETF RFC 1493, Definitions of Managed Objects for Bridges.
- [28] IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).
- [29] IETF RFC 2011, SNMPv2 MIB for the Internet Protocol Using SMIv2.
- [30] IETF RFC 2013, SNMPv2 MIB for the User Datagram Protocol Using SMIv2.
- [31] IETF RFC 3665, Definitions of Managed Objects for the Ethernet-like Interface Types, September 2003.
- [32] IETF RFC 2959, Real-Time Transport Protocol Management Information Base
- [33] PacketCable 1.5 Audio/Video Codec Specification, PKT-SP-CODEC1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.
- [34] PacketCable 1.5 Management Event MIB Specification, PKT-SP-EVEMIB1.5-I01-050128, January 28, 2005, Cable Television Laboratories, Inc.

## 2.3 Reference Acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone 303-661-9100; Fax 303-661-9199; Internet: [www.packetcable.com/](http://www.packetcable.com/) or [www.cablemodem.com](http://www.cablemodem.com).
- IETF RFCs: [www.ietf.org/](http://www.ietf.org/)



### 3 TERMS AND DEFINITIONS

PacketCable specifications use the following terms:

<b>Access Control</b>	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes, or other system resources on a network.
<b>Active</b>	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.
<b>Admitted</b>	A service flow is said to be "admitted" when the CMTS has reserved resources (e.g., bandwidth) for it on the DOCSIS network.
<b>A-link</b>	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access."
<b>Asymmetric Key</b>	An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct.
<b>Audio Server</b>	An Audio Server plays informational announcements in PacketCable 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.
<b>Authentication</b>	The process of verifying the claimed identity of an entity to another entity.
<b>Authenticity</b>	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.
<b>Authorization</b>	The act of giving access to a service or device if one has permission to have the access.
<b>Cipher</b>	An algorithm that transforms data between plaintext and ciphertext.
<b>Ciphersuite</b>	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 PacketCable.
<b>Ciphertext</b>	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
<b>Cleartext</b>	The original (unencrypted) state of a message or data. Also called plaintext.
<b>Confidentiality</b>	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.
<b>Cryptanalysis</b>	The process of recovering the plaintext of a message or the encryption key without access to the key.
<b>Cryptographic algorithm</b>	An algorithm used to transfer text between plaintext and ciphertext.
<b>Decipherment</b>	A procedure applied to ciphertext to translate it into plaintext.
<b>Decryption</b>	A procedure applied to ciphertext to translate it into plaintext.
<b>Decryption key</b>	The key in the cryptographic algorithm to translate the ciphertext to plaintext.
<b>Digital certificate</b>	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate.

<b>Digital signature</b>	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.
<b>Downstream</b>	The direction from the headend toward the subscriber location.
<b>Encipherment</b>	A method used to translate plaintext into ciphertext.
<b>Encryption</b>	A method used to translate plaintext into ciphertext.
<b>Encryption Key</b>	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
<b>Endpoint</b>	A Terminal, Gateway or Multipoint Conference Unit (MCU).
<b>Errored Second</b>	Any 1-second interval containing at least one bit error.
<b>Event Message</b>	A message capturing a single portion of a connection.
<b>F-link</b>	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
<b>Flow [DOCSIS Flow]</b>	(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.
<b>Flow [IP Flow]</b>	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.
<b>Gateway</b>	Devices bridging between the PacketCable 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 PacketCable network.
<b>H.323</b>	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.
<b>Header</b>	Protocol control information located at the beginning of a protocol data unit.
<b>Integrity</b>	A way to ensure that information is not modified except by those who are authorized to do so.
<b>IntraLATA</b>	Within a Local Access Transport Area.
<b>Jitter</b>	Variability in the delay of a stream of incoming packets making up a flow such as a voice communication.
<b>Kerberos</b>	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
<b>Key</b>	A mathematical value input into the selected cryptographic algorithm.
<b>Key Exchange</b>	The swapping of public keys between entities to be used to encrypt communication between the entities.
<b>Key Management</b>	The process of distributing shared symmetric keys needed to run a security protocol.
<b>Key Pair</b>	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.

<b>Keying Material</b>	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
<b>Keyspace</b>	The range of all possible values of the key for a particular cryptographic algorithm.
<b>Latency</b>	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
<b>Link Encryption</b>	Cryptography applied to data as it travels on data links between the network devices.
<b>Network Layer</b>	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
<b>Network Management</b>	The functions related to the management of data across the network.
<b>Network Management OSS</b>	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.
<b>Nonce</b>	A random value used only once that is sent in a communications protocol exchange to prevent replay attacks.
<b>Non-Repudiation</b>	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
<b>Off-Net Call</b>	A communication connecting a PacketCable subscriber out to a user on the PSTN.
<b>On-Net Call</b>	A communication placed by one customer to another customer entirely on the PacketCable Network.
<b>One-way Hash</b>	A hash function that has an insignificant number of collisions upon output.
<b>Plaintext</b>	The original (unencrypted) state of a message or data. Also called cleartext.
<b>Pre-shared Key</b>	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
<b>Privacy</b>	A way to ensure that information is not disclosed to any one other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
<b>Private Key</b>	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
<b>Proxy</b>	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.
<b>Public Key</b>	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.
<b>Public Key Certificate</b>	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
<b>Public Key Cryptography</b>	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.

<b>Root Private Key</b>	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.
<b>Root Public Key</b>	The public key of the highest level Certification Authority, normally used to verify digital signatures generated with the corresponding root private key.
<b>Secret Key</b>	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.
<b>Session Key</b>	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
<b>Signed and Sealed</b>	An "envelope" of information which has been signed with a digital signature and sealed using encryption.
<b>Subflow</b>	A unidirectional flow of IP packets characterized by a single source and destination IP address and single source and destination UDP/TCP port.
<b>Symmetric Key</b>	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.
<b>Systems Management</b>	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.
<b>Transit Delays</b>	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.
<b>Trunk</b>	An analog or digital connection from a circuit switch that carries user media content and may carry voice signaling ( $M_F$ , $R_2$ , etc.).
<b>Tunnel Mode</b>	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.
<b>Upstream</b>	The direction from the subscriber location toward the headend.
<b>X.509 certificate</b>	A public key certificate specification developed as part of the ITU-T X.500 standards directory

## 4 ABBREVIATIONS

PacketCable specifications use the following abbreviations.

<b>AAA</b>	Authentication, Authorization and Accounting.
<b>AES</b>	Advanced Encryption Standard. A block cipher, used to encrypt the media traffic in PacketCable.
<b>AF</b>	Assured Forwarding. This is a DiffServ Per Hop Behavior.
<b>AH</b>	Authentication header. An IPsec security protocol that provides message integrity for complete IP packets, including the IP header.
<b>AMA</b>	Automated Message Accounting. A standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies).
<b>ASD</b>	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.
<b>AT</b>	Access Tandem.
<b>ATM</b>	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
<b>BAF</b>	Bellcore AMA Format, also known as AMA.
<b>BCID</b>	Billing Correlation ID.
<b>BPI+</b>	Baseline Privacy Plus Interface Specification. The security portion of the DOCSIS 1.1 standard that runs on the MAC layer.
<b>CA</b>	Certification Authority. A trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
<b>CA</b>	Call Agent. The part of the CMS that maintains the communication state, and controls the line side of the communication.
<b>CBC</b>	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.
<b>CBR</b>	Constant Bit Rate.
<b>CDR</b>	Call Detail Record. A single CDR is generated at the end of each billable activity. A single billable activity may also generate multiple CDRs.
<b>CIC</b>	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.
<b>CID</b>	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.
<b>CIF</b>	Common Intermediate Format.
<b>CIR</b>	Committed Information Rate.
<b>CM</b>	DOCSIS Cable Modem.
<b>CMS</b>	Cryptographic Message Syntax.

<b>CMS</b>	Call Management Server. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology. This is one example of an Application Server.
<b>CMTS</b>	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.
<b>CMSS</b>	Call Management Server Signaling.
<b>Codec</b>	COder-DECoder.
<b>COPS</b>	Common Open Policy Service protocol. Defined in RFC2748.
<b>CoS</b>	Class of Service. The type 4 tuple of a DOCSIS configuration file.
<b>CRCX</b>	Create Connection.
<b>CSR</b>	Customer Service Representative.
<b>DA</b>	Directory Assistance.
<b>DE</b>	Default. This is a DiffServ Per Hop Behavior.
<b>DES</b>	Data Encryption Standard.
<b>DF</b>	Delivery Function.
<b>DHCP</b>	Dynamic Host Configuration Protocol.
<b>DHCP-D</b>	DHCP Default. Network Provider DHCP Server.
<b>DNS</b>	Domain Name Service.
<b>DOCSIS®</b>	Data-Over-Cable Service Interface Specifications.
<b>DPC</b>	Destination Point Code. In ANSI SS7, a 3-octet number which uniquely identifies an SS7 Signaling Point, either an SSP, STP, or SCP.
<b>DQoS</b>	Dynamic Quality-of-Service. Assigned on the fly for each communication depending on the QoS requested.
<b>DSA</b>	Dynamic Service Add.
<b>DSC</b>	Dynamic Service Change.
<b>DSCP</b>	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.
<b>DTMF</b>	Dual-tone Multi Frequency (tones).
<b>EF</b>	Expedited Forwarding. A DiffServ Per Hop Behavior.
<b>E-MTA</b>	Embedded MTA. A single node that contains both an MTA and a cable modem.
<b>EO</b>	End Office.
<b>ESP</b>	IPsec Encapsulating Security Payload. Protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
<b>ETSI</b>	European Telecommunications Standards Institute.
<b>F-link</b>	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
<b>FEID</b>	Financial Entity ID.
<b>FGD</b>	Feature Group D signaling.
<b>FQDN</b>	Fully Qualified Domain Name. Refer to IETF RFC 2821 for details.
<b>GC</b>	Gate Controller.
<b>GTT</b>	Global Title Translation.

<b>HFC</b>	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.
<b>HMAC</b>	Hashed Message Authentication Code. A message authentication algorithm, based on either SHA-1 or MD5 hash and defined in IETF RFC 2104.
<b>HTTP</b>	Hypertext Transfer Protocol. Refer to IETF RFC 1945 and RFC 2068.
<b>IANA</b>	Internet Assigned Numbered Authority. See <a href="http://www.ietf.org">www.ietf.org</a> for details.
<b>IC</b>	Inter-exchange Carrier.
<b>IETF</b>	Internet Engineering Task Force. A body responsible, among other things, for developing standards used on the Internet. See <a href="http://www.ietf.org">www.ietf.org</a> for details.
<b>IKE</b>	Internet Key Exchange. A key-management mechanism used to negotiate and derive keys for SAs in IPsec.
<b>IKE–</b>	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
<b>IKE+</b>	A notation defined to refer to the use of IKE with X.509 certificates for authentication.
<b>IP</b>	Internet Protocol. An Internet network-layer protocol.
<b>IPsec</b>	Internet Protocol Security. A collection of Internet standards for protecting IP packets with encryption and authentication.
<b>ISDN</b>	Integrated Services Digital Network.
<b>ISTP</b>	Internet Signaling Transport Protocol.
<b>ISUP</b>	ISDN User Part. A protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
<b>ITU</b>	International Telecommunication Union.
<b>ITU-T</b>	International Telecommunication Union–Telecommunication Standardization Sector.
<b>IVR</b>	Interactive Voice Response system.
<b>KDC</b>	Key Distribution Center.
<b>LATA</b>	Local Access and Transport Area.
<b>LD</b>	Long Distance.
<b>LIDB</b>	Line Information Database. Contains customer information required for real-time access such as calling card personal identification numbers (PINs) for real-time validation.
<b>LLC</b>	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.
<b>LNP</b>	Local Number Portability. Allows a customer to retain the same number when switching from one local service provider to another.
<b>LSSGR</b>	LATA Switching Systems Generic Requirements.
<b>MAC</b>	Message Authentication Code. A fixed-length data item that is sent together with a message to ensure integrity, also known as a MIC.
<b>MAC</b>	Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
<b>MC</b>	Multipoint Controller.
<b>MCU</b>	Multipoint Conferencing Unit.
<b>MD5</b>	Message Digest 5. A one-way hash algorithm that maps variable length plaintext into fixed-length (16 byte) ciphertext.

<b>MDCP</b>	Media Device Control Protocol. A media gateway control specification submitted to IETF by Lucent. Now called SCTP.
<b>MDCX</b>	Modify Connection.
<b>MDU</b>	Multi-Dwelling Unit. Multiple units within the same physical building. The term is usually associated with high-rise buildings.
<b>MEGACO</b>	Media Gateway Control IETF working group. See <a href="http://www.ietf.org">www.ietf.org</a> for details.
<b>MF</b>	Multi-Frequency.
<b>MG</b>	Media Gateway. Provides the bearer circuit interfaces to the PSTN and transcodes the media stream.
<b>MGC</b>	Media Gateway Controller. The overall controller function of the PSTN gateway. Receives, controls and mediates call-signaling information between the PacketCable and PSTN.
<b>MGCP</b>	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF 2705.
<b>MIB</b>	Management Information Base.
<b>MIC</b>	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).
<b>MMC</b>	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
<b>MSB</b>	Most Significant Bit.
<b>MSO</b>	Multi-System Operator. A cable company that operates many headend locations in several cities.
<b>MSU</b>	Message Signal Unit.
<b>MTA</b>	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.
<b>MTP</b>	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.
<b>MWD</b>	Maximum Waiting Delay.
<b>NANP</b>	North American Numbering Plan.
<b>NANPNAT</b>	North American Numbering Plan Network Address Translation.
<b>NAT Network Layer</b>	Network Address Translation. Layer 3 in the Open System Interconnection (OSI) architecture. This layer provides services to establish a path between open systems.
<b>NCS</b>	Network Call Signaling.
<b>NPA-NXX</b>	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).
<b>NTP</b>	Network Time Protocol. An internet standard used for synchronizing clocks of elements distributed on an IP network.
<b>NTSC</b>	National Television Standards Committee. Defines the analog color television broadcast standard used today in North America.
<b>OID</b>	Object Identification.
<b>OSP</b>	Operator Service Provider.



<b>OSS</b>	Operations Systems Support. The back-office software used for configuration, performance, fault, accounting, and security management.
<b>OSS-D</b>	OSS Default. Network Provider Provisioning Server.
<b>PAL</b>	Phase Alternate Line. The European color television format that evolved from the American NTSC standard.
<b>PCES</b>	PacketCable Electronic Surveillance.
<b>PCM</b>	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.
<b>PDU</b>	Protocol Data Unit.
<b>PHS</b>	Payload Header Suppression. A DOCSIS technique for compressing the Ethernet, IP, and UDP headers of RTP packets.
<b>PKCROSS</b>	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).
<b>PKCS</b>	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.
<b>PKI</b>	Public-Key Infrastructure. A process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
<b>PKINIT</b>	Public-Key Cryptography for Initial Authentication. The extension to the Kerberos protocol that provides a method for using public-key cryptography during initial authentication.
<b>PSC</b>	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
<b>PSFR</b>	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
<b>PSTN</b>	Public Switched Telephone Network.
<b>QCIF</b>	Quarter Common Intermediate Format.
<b>QoS</b>	Quality of Service. Guarantees network bandwidth and availability for applications.
<b>RADIUS</b>	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.
<b>RAS</b>	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
<b>RC4</b>	Rivest Cipher 4. A variable length stream cipher. Optionally used to encrypt the media traffic in PacketCable.
<b>RFC</b>	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at <a href="http://www.ietf.cnri.reston.va.us/rfc.html">http://www.ietf.cnri.reston.va.us/rfc.html</a> .
<b>RFI</b>	The DOCSIS Radio Frequency Interface specification.
<b>RJ-11</b>	Registered Jack-11. A standard 4-pin modular connector commonly used in the United States for connecting a phone unit into a wall jack.

<b>RKS</b>	Record Keeping Server. The device, which collects and correlates the various Event Messages.
<b>RSA</b>	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.
<b>RSA Key Pair</b>	A public/private key pair created for use with the RSA cryptographic algorithm.
<b>RTCP</b>	Real-Time Control Protocol.
<b>RTO</b>	Retransmission Timeout.
<b>RTP</b>	Real-time Transport Protocol. A protocol for encapsulating encoded voice and video streams. Refer to IETF RFC 1889.
<b>SA</b>	Security Association. A one-way relationship between sender and receiver offering security services on the communication flow.
<b>SAID</b>	Security Association Identifier. Uniquely identifies SAs in the DOCSIS Baseline Privacy Plus Interface (BPI+) security protocol.
<b>SCCP</b>	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.
<b>SCP</b>	Service Control Point. A Signaling Point within the SS7 network, identifiable by a Destination Point Code that provides database services to the network.
<b>SCTP</b>	Stream Control Transmission Protocol.
<b>SDP</b>	Session Description Protocol.
<b>SDU</b>	Service Data Unit. Information delivered as a unit between peer service access points.
<b>SF</b>	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
<b>SFID</b>	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.
<b>SFR</b>	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.
<b>SG</b>	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.
<b>SGCP</b>	Simple Gateway Control Protocol. Earlier draft of MGCP.
<b>SHA – 1</b>	Secure Hash Algorithm 1. A one-way hash algorithm.
<b>SID</b>	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.
<b>SIP</b>	Session Initiation Protocol. An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.

<b>SIP+</b>	Session Initiation Protocol Plus. An extension to SIP.
<b>S-MTA</b>	Standalone MTA. A single node that contains an MTA and a non-DOCSIS MAC (e.g., ethernet).
<b>SNMP</b>	Simple Network Management Protocol.
<b>SOHO</b>	Small Office/Home Office.
<b>SS7</b>	Signaling System number 7. An architecture and set of protocols for performing out-of-band call signaling with a telephone network.
<b>SSP</b>	Service Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
<b>STP</b>	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.
<b>TCAP</b>	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling Control Point.
<b>TCP</b>	Transmission Control Protocol.
<b>TD</b>	Timeout for Disconnect.
<b>TFTP</b>	Trivial File Transfer Protocol.
<b>TFTP-D</b>	Default – Trivial File Transfer Protocol.
<b>TGS</b>	Ticket Granting Server. A sub-system of the KDC used to grant Kerberos tickets.
<b>TGW</b>	Telephony Gateway.
<b>TIPHON</b>	Telecommunications and Internet Protocol Harmonization Over Network.
<b>TLV</b>	Type-Length-Value. A tuple within a DOCSIS configuration file.
<b>TN</b>	Telephone Number.
<b>ToD</b>	Time-of-Day Server.
<b>TOS</b>	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.
<b>TSG</b>	Trunk Subgroup.
<b>UDP</b>	User Datagram Protocol. A connectionless protocol built upon Internet Protocol (IP).
<b>VAD</b>	Voice Activity Detection.
<b>VBR</b>	Variable Bit Rate.
<b>VoIP</b>	Voice-over-IP.

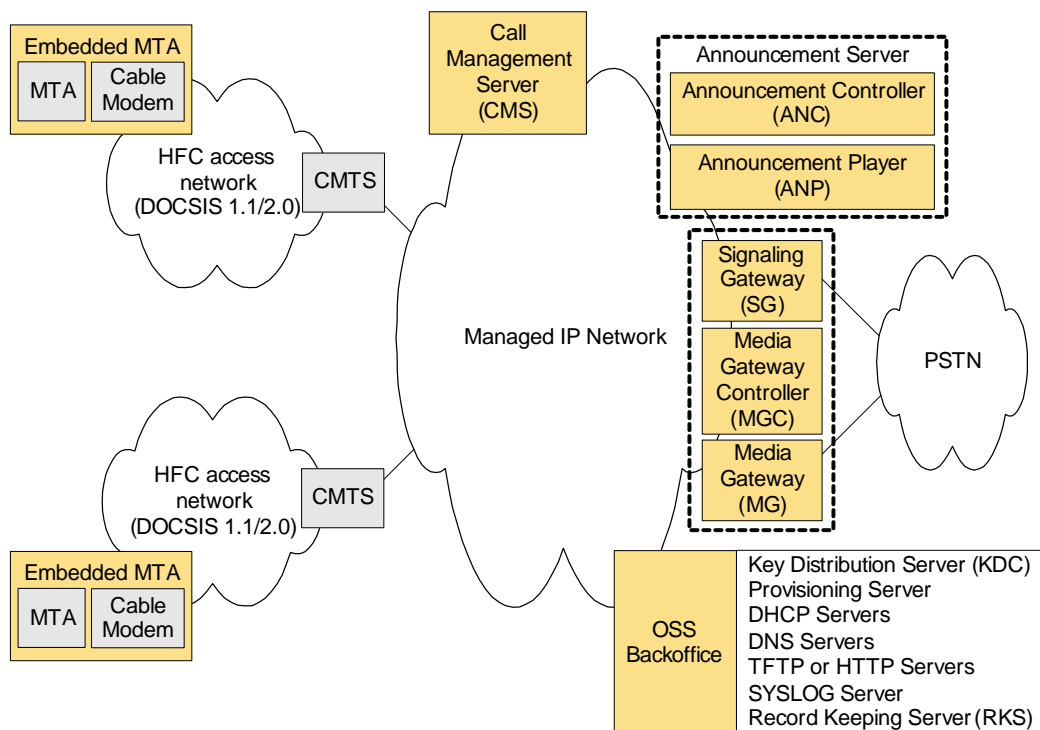
## 5 OVERVIEW

PacketCable MIB modules are designed to provide necessary functionality defined in PacketCable 1.5 specifications. The MIB design follows the same multi-phase schedule as the rest of PacketCable specifications. Table 1 lists PacketCable functional areas that are in scope of PacketCable 1.5.

### 5.1 PacketCable Reference Architecture

The conceptual diagram for the PacketCable architecture is shown in Figure 1

Please refer to the architecture document [1] for more detailed information concerning the PacketCable architecture.



**Figure 1. PacketCable Reference Architecture**

### 5.2 General Requirements

The PacketCable MIBs Framework Specification follows the Internet Standard Management Framework described in RFC 3410 [20]. Additionally, the following requirements have been considered in the design of the PacketCable MIB modules.

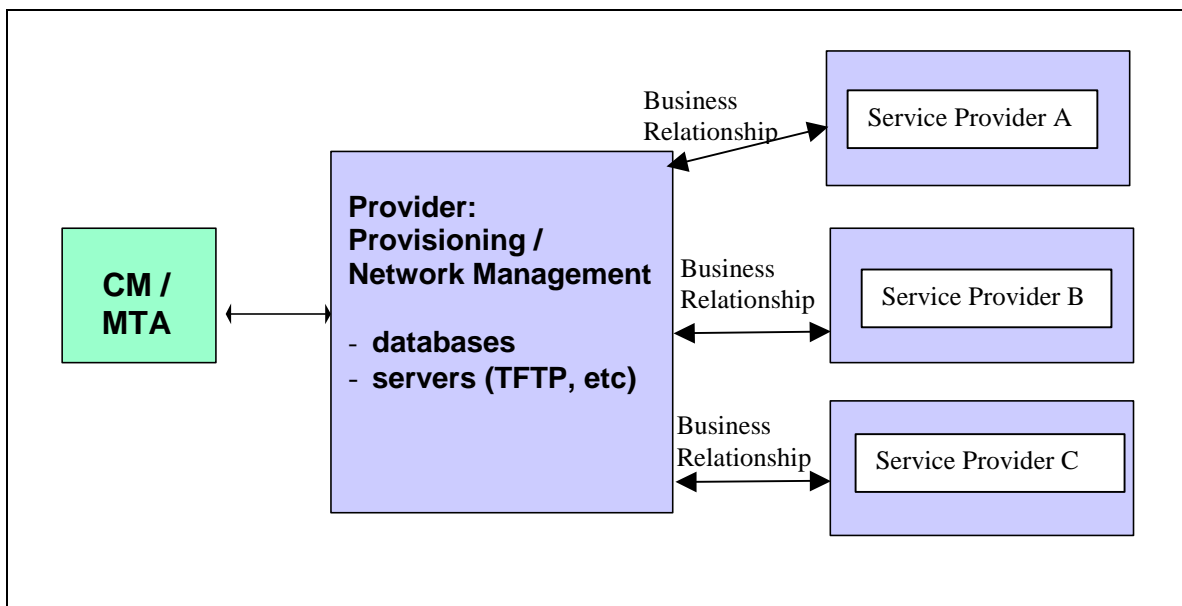
- PacketCable devices must be compliant with DOCSIS 1.1 or DOCSIS 2.0; therefore PacketCable devices **MUST** support DOCSIS 1.1 or DOCSIS 2.0 MIBs as defined in section 6.1 of this document.
- Take a minimalist approach for design of the PacketCable MIB modules, i.e., if other MIB modules define the same functions, then rely on these MIB modules rather than create new ones.
- Organize MIB modules to support Embedded MTA (E-MTA).

- Organize MIB modules so as to allow functional partitioning of DOCSIS (high-speed data) and PacketCable (voice) features.
- DOCSIS 1.1 or DOCSIS 2.0 within PacketCable applications requires support of SNMPv3 and SNMPv2; therefore PacketCable MIB agents MUST comply with SNMPv3 and SNMPv2.
- PacketCable MIB modules MUST comply with SMIPv2 as defined in IETF STD 58 [26].

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., E-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.

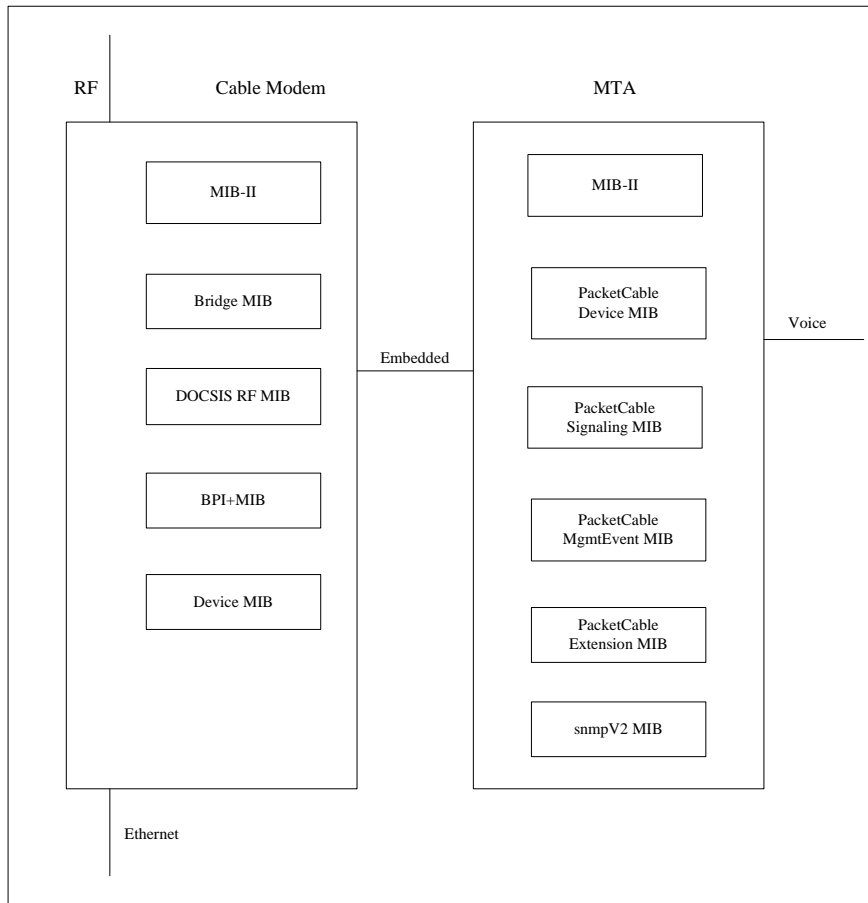


**Figure 2. Partitioning of Management Domains**

### 5.2.2 Support for Embedded MTAs

The PacketCable MIB modules include features for E-MTAs. Since the E-MTAs are not required to support any DOCSIS related functions, they MUST NOT share any MIB objects in common with DOCSIS. The PacketCable MIB modules are, however, designed to provide management support for voice related functions. DOCSIS Cable Modems with E-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 E-MTA:

**MTA MIB Implementation****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.

PacketCable MIB modules **MUST** conform to SMIV2 [26]

The following IETF RFCs provide more information on SNMPv3: 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 the Simple Network Management Protocol (SNMP) [25].

### 5.2.3.1 USM Requirements

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 E-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 PacketCable. Other table entries MAY be implemented at vendor or operator discretion.

VACM views MUST be defined for PacketCable 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 E-MTA, write access to PacketCable MIB modules, and notifications as defined in the PacketCable MIB modules:

```
vacmGroupName - PacketCableFullAccess
vacmAccessContextPrefix - ""
vacmAccessSecurityModel - USM
vacmAccessSecurityLevel - authPriv or authNoPriv, depending on whether
privacy has been specified
vacmAccessContextMatch - exact
vacmAccessReadOnlyViewName - ReadOnlyView
vacmAccessWriteViewName - FullAccessView
vacmAccessNotifyViewName - 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 PacketCable 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 PacketCable defined MIB modules, and vendor defined MIB modules for PacketCable.

```
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 PacketCable MIB modules.

### 5.3.1 PacketCable Device Provisioning

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

### 5.3.2 Security

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

### 5.3.3 Voice interfaces

PacketCable 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 PacketCable Voice Call Signaling

The PacketCable 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 PacketCable 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 PacketCable [33]. The RTP MIB (IETF RFC 2959 [32]) may be used for management of the media transport function of the E-MTA but this is considered out of scope for PacketCable.

### 5.3.6 Fault Management

The PacketCable 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 PacketCable MTA MIB [12], the PacketCable Signaling MIB [13], and Management Event MIB [34] specifications. Further definition of default management is out of scope of PacketCable.

### 5.3.7 Performance Management

The PacketCable 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 PacketCable.

### 5.3.8 Event Management

The PacketCable Management Event MIB module provides the means to define and distribute events generated by the E-MTA. This provides the ability for vendors to define their own events as well as support

of PacketCable defined events. These events should support modifiable attributes such as priority level. The PacketCable MIB should allow the ability to log events by a variety of means like local log, syslog, SNMP Traps and SNMP INFORMs. Refer to [34] for more details.

## 6 MIB MODULES AVAILABLE IN A PACKETCABLE NETWORK

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

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

**Table 2. MIB modules implemented by E-MTA**

IF MIB
MIB II
Ethernet MIB
Bridge MIB
PacketCable MTA Device MIB
PacketCable Signaling MIB
PacketCable Management Event MIB
snmpV2 MIB group
PacketCable Extension MIB

As mentioned before, partitioning of voice and data services and support of E-MTA has been part of the requirements for design of the PacketCable 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 PacketCable E-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 [5].
- For DOCSIS 2.0, the MIB module requirements are defined in [11].

### 6.2 IF MIB

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

### 6.3 MIB II

RFC 1907, RFC 2011, and RFC 2013 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 E-MTA device. The PacketCable MIB module only requires the **system**, **interfaces**, **IP**, and **transmission** objects of MIB II to be present in the E-MTA.

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

#### 6.3.1 sysDescr Requirements

The E-MTA's MIB II sysDescr object **MUST** conform to the format specified in DOCSIS OSS1 [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 E-MTA.

### 6.3.3 "ifTable" Requirements

PacketCable ifTable MUST contain information about all PacketCable endpoints. IfIndex 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 CableModem part of an E-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 PacketCable 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 E-MTA the tables 3 and 4 MUST be adhered to.

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

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

<b>RFC-2863 MIB-Object Details for E-MTA Device Interface</b>	<b>MTA Device</b>
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 E-MTA Device Interfaces**

<b>RFC-2011 MIB-Object details for E-MTA Devices Interfaces</b>	<b>CM device</b>
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 [31]).

## 6.5 PacketCable SIGNALING MIB

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

The PacketCable Signaling MIB module contains general configuration information that applies to the Network Call Signaling (NCS) protocol [17] on a per MTA device basis. This data only provides the means to provision call signaling parameters on a device basis.

The PacketCable Signaling MIB module also defines managed objects applicable on a per endpoint basis. The NCS endpoint table (`pkcSigEndPntConfigTable`) 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 PacketCable NCS specification [17]. This data only provides the means to provision network call signaling per endpoint.

## 6.6 PacketCable MTA MIB module

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

The PacketCable 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.

## 6.7 Event Management MIB

The PacketCable Management Event MIB module is defined in [34]. It provides a common data and format definition for events (informative, alarm, etc). It also specifies by what means events are transmitted. Use of a common event mechanism facilitates management of the E-MTA in a multi-vendor environment and provides a standard means to implement PacketCable specified events.

## 6.8 SNMP MIB

The SNMPv2 MIB module defines the functionality to configure the endpoint in SNMPv2 mode and helps in managing all the MIB objects using SNMPv2 functionality.

## 6.9 PacketCable Extension MIB

The PacketCable Extension MIB is defined in [10]. These MIBs are extending the existing PacketCable1.0 MIB functionality. The extensions are in the areas of MTA MIB and Signaling MIB. .

**6.9.1 MTA MIB Extension:**

The PacketCable MTA MIB Extension is defined in [14]. This provides the additional functionality for controlling new functionality like Multiple Grants Per Interval (MGPPi) on the endpoint

**6.9.2 Signaling MIB Extension**

The PacketCable Signaling MIB Extension is defined in [13]. This provides additional control and reporting functionality for endpoints in the areas of DTMF relay, Quarantine handling, Hookstate etc.

**6.9.3 Syslog MIB**

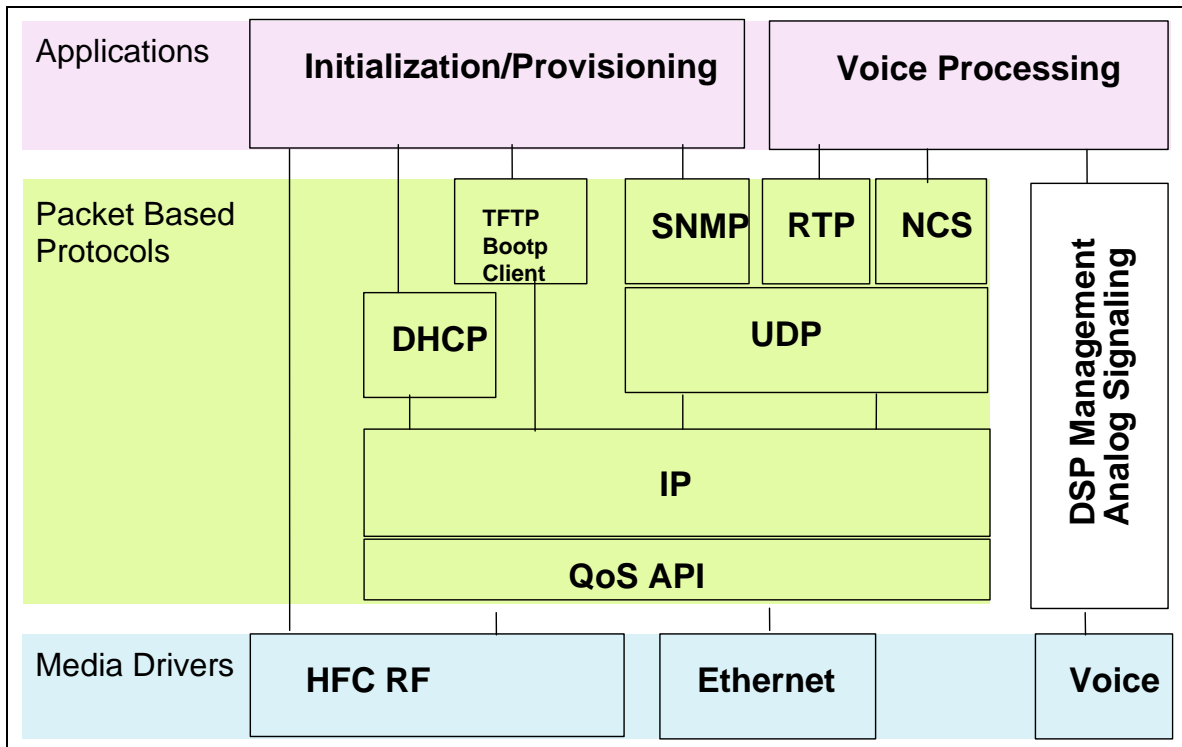
This Syslog MIB is defined in [34]. This provides a better granularity for control of syslog messages by the endpoint.

## 7 PACKETCABLE MIB MODULE IMPLEMENTATION

This section describes a reference implementation of the MIB modules in a PacketCable device. Only E-MTA is considered in this section.

### 7.1 MTA components

Figure 4 below shows the components of a typical E-MTA.



**Figure 4. E-MTA Components**

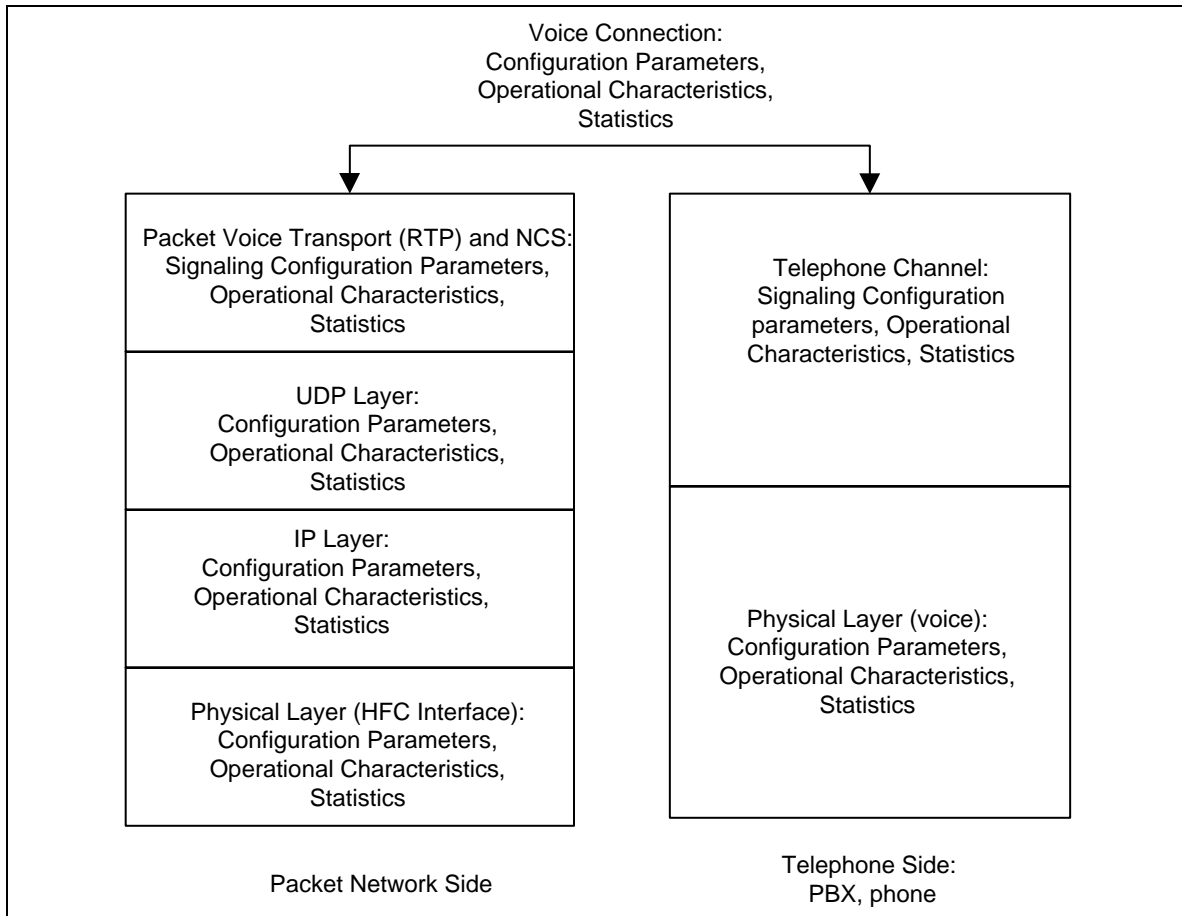
As shown here the E-MTA components can be organized into separate areas, i.e., packet based protocols, which run on top of IP and the voice subsystem, which consists of DSP engines and their associated software. MIB modules that are implemented in the MTA have to be organized so as to facilitate this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

Note: Please refer to the PacketCable Security Specification [18] 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.

## Appendix A. Acknowledgements

The PacketCable project would like to acknowledge the members of the PacketCable OSS focus group whose efforts have been invaluable for creation of this document. In particular we wish to recognize and thank the following for their contribution to this document:

Angela Lyda (Arris Interactive)  
Rick Morris (Arris Interactive)  
Klaus Hermanns (Cisco Systems, Inc.)  
Eugene Nechamkin (Broadcom Corp.)  
Rick Vetter (Motorola, Inc.)  
Roy Spitzer (Telogy/TI)  
Satish Kumar (Texas Instruments)

*Jean-Francois Mule, Sumanth Channabasappa, Venkatesh Sunkad (CableLabs, Inc.)*