

Superseded

PacketCable™ MIBs Framework Specification

PKT-SP-MIBS-I05-021127

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 1999 - 2002 Cable Television Laboratories, Inc.
All rights reserved.

Document Status Sheet

| | | | |
|-----------------------------------|--|----------------------|--|
| Document Control Number: | PKT-SP-MIBS-I05-021127 | | |
| Document Title: | PacketCable™ MIBs Framework Specification | | |
| Revision History: | I01 — Issued December 1, 1999 I02 — Issued March 23, 2001 I03 — Issued January 16, 2002 I04 — Issued October 18, 2002 I05 — Issued November 27, 2002 | | |
| Date: | November 27, 2002 | | |
| Status: | Work in Progress | Draft | Issued |
| Distribution Restrictions: | Author Only | GL/Member | GL/ PacketCable/ Vendor Public |

Key to Document Status Codes:

| | |
|-------------------------|--|
| Work in Progress | An incomplete document designed to guide discussion and generate feedback, which may include several alternative requirements for consideration. |
| Draft | 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. |
| Issued | 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. |
| Closed | A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs. |

Contents

| | |
|--|-----------|
| 1 INTRODUCTION..... | 1 |
| 1.1 Purpose..... | 1 |
| 1.2 Specification Language..... | 2 |
| 2 REFERENCES (NORMATIVE)..... | 3 |
| 3 TERMS AND DEFINITIONS | 4 |
| 4 ABBREVIATIONS | 8 |
| 5 OVERVIEW..... | 14 |
| 5.1 PacketCable Reference Architecture..... | 14 |
| 5.2 General Requirements..... | 14 |
| 5.2.1 Provisioning and Network Management Service Provider..... | 15 |
| 5.2.2 Support for Embedded and Standalone MTAs | 15 |
| 5.2.3 SNMP Considerations | 16 |
| 5.3 Functional Requirements..... | 18 |
| 5.3.1 PacketCable Device Provisioning | 18 |
| 5.3.2 Security | 18 |
| 5.3.3 QoS (For consideration in future releases of PacketCable)..... | 18 |
| 5.3.4 Primary Line Requirements (For consideration in future releases of PacketCable)..... | 19 |
| 5.3.5 Voice interfaces..... | 19 |
| 5.3.6 Packet Voice Call Signaling | 19 |
| 5.3.7 Packet Voice Transport (For consideration in future releases of PacketCable) | 19 |
| 5.3.8 Fault Management (For consideration in future releases of PacketCable)..... | 19 |
| 5.3.9 Performance Management (For consideration in future releases of PacketCable)..... | 20 |
| 5.3.10 Event Management | 20 |
| 6 MIBS AVAILABLE IN A PACKETCABLE NETWORK..... | 21 |
| 6.1 DOCSIS 1.1 MIBs..... | 21 |
| 6.2 IF MIB | 21 |
| 6.3 MIB II..... | 22 |
| 6.3.1 sysDescr Requirements | 22 |
| 6.3.2 sysObjectID Requirements | 22 |
| 6.3.3 “iftable” Requirements | 22 |
| 6.4 Ethernet MIB..... | 25 |
| 6.5 Bridge MIB | 25 |
| 6.6 PacketCable MTA SIGNALING MIB | 25 |
| 6.6.1 MTA SIGNALING MIB general configuration information | 25 |
| 6.6.2 MTA NCS MIB per endpoint data..... | 25 |

6.7 PacketCable MTA Device MIB 25
 6.7.1 MTA Device MIB general configuration information..... 26
 6.7.2 MTA Device MIB Syslog Information 26

6.8 Event Management MIB..... 26

7 PACKETCABLE MIB IMPLEMENTATION 27

7.1 MTA components..... 27

7.2 MIB Layering 27

APPENDIX A. CABLELABS MIB IMPORT DATA 29

APPENDIX B. BIBLIOGRAPHY INFORMATIVE 31

APPENDIX C. ACKNOWLEDGEMENTS 32

APPENDIX D. REVISIONS 33

Figures

Figure 1. PacketCable Reference Architecture 14

Figure 2. Partitioning of Management Domains 15

Figure 3. Embedded and Standalone MTA implementations 16

Figure 4. MTA Components 27

Figure 5. MIB Layering Model 28

Tables

Table 1: Functional MIB Areas 1

Table 2: Additional MIBs 21

Table 3 RFC 2863 ifTable, MIB-Object Details for embedded MTA Device Interfaces..24

Table 4. RFC 2011 ipNetToMedia MIB-Object Details for eMTA Device Interfaces25

1 INTRODUCTION

1.1 Purpose

This specification describes the framework in which PacketCable™ MIBs (Management Information Base) are defined. It provides information on the management requirements of PacketCable specified devices and networks and how these requirements are supported in the MIB. It is intended to support and complement the original MIBs in which these requirements are defined. 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

| PacketCable Specification | Phase | MIB development |
|----------------------------------|------------|--|
| DCS Signaling | Future | TBD |
| Inter-Domain CMS – CMS Signaling | Future | TBD |
| NCS Signaling | 1.0/Future | MTA SIGNALING MIB Telephony config file CMS SIGNALING MIB (Future) |
| Device Provisioning | 1.0 | MTA Device MIB Telephony config file |
| Management Event Mechanism | 1.0 | Management Event MIB |
| Primary Line | Future | TBD |
| Packet Voice transport | Future | TBD |
| Codec | 1.0/Future | MTA SIGNALING MIB |
| Security | 1.0 | MTA Device MIB Telephony config file |
| Performance | Future | Incorporation of RTP MIB Additions to SIGNALING MIB |
| D-QoS | Future | TBD |
| LAESS | Future | TBD |

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 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)

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 Architecture Framework, PKT-TR-ARCH-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., <http://www.packetcable.com>.
- [2] PacketCable MTA Device Provisioning Specification, PKT-SP-PROV-I05-021127, November 27, 2002, Cable Television Laboratories, Inc., <http://www.packetcable.com>.
- [3] IETF RFC 2571 An Architecture for Describing SNMP Management Framework, B. Wijnen, D. Harrington, R. Presuhn, April 1999.
- [4] *Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems*, IETF RFC 2669.
- [5] *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces*, IETF RFC 2670.
- [6] Data Over Cable System Quality of Service Management Information Base (DOCSIS-QOS MIB), draft-ietf-ipcdn-qos-mib-04.txt.
- [7] Data Over Cable System Operations Support System Interface, SP-OSSIV1.1-I06-020830, August 30, 2002, Cable Television Laboratories, Inc., <http://www.packetcable.com>.
- [8] INTERNET PROTOCOL, IETF RFC791, <http://www.ietf.org/rfc/rfc791.txt>
- [9] INTERNET CONTROL MESSAGE PROTOCOL, IETF RFC792, <http://www.ietf.org/rfc/rfc792.txt>
- [10] SNMPv2 Management Information Base for the Internet Protocol using SMIV2, IETF RFC 2011, <http://www.ietf.org/rfc/rfc2011.txt>.
- [11] The Interfaces Group MIB, IETF RFC2863, <http://www.ietf.org/rfc/rfc2011.txt>
- [12] eDOCSIS™ Specification, SP-eDOCSIS-D02-021127, CableLabs.

3 TERMS AND DEFINITIONS

PacketCable specifications use the following terms:

| | |
|--------------------------------|---|
| Access Control | Limiting the flow of information from the resources of a system only to authorized persons, programs, processes, or other system resources on a network. |
| Active | A service flow is said to be “active” when it is permitted to forward data packets. A service flow must first be admitted before it is active. |
| Admitted | A service flow is said to be “admitted” when the CMTS has reserved resources (e.g., bandwidth) for it on the DOCSIS network. |
| A-link | A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. ‘A’ stands for “Access.” |
| Asymmetric Key | An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct. |
| Audio Server | An Audio Server plays informational announcements in 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. |
| 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 PacketCable. |
| 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 head-end 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. |
| 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 unidirectional sequence of packets associated with a Service ID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow. Also known as a DOCSIS-QoS "service 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 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. |
| 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 and 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 a PacketCable subscriber to a user on the PSTN. |
| One-way Hash | A hash function that has an insignificant number of collisions upon output. |
| On-Net Call | A communication placed by one customer to another customer entirely on the PacketCable Network. |
| 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 any one 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

PacketCable specifications use the following abbreviations.

| | |
|--------------|---|
| AAA | Authentication, Authorization and Accounting |
| AES | Advanced Encryption Standard. A block cipher, used to encrypt the media traffic in PacketCable. |
| 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 head-end which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network. |
| CMSS | CMS-to-CMS Signaling |
| Codec | COder-DECoder |
| COPS | Common Open Policy Service protocol. Currently an internet draft, which describes a client/server model for supporting policy control over QoS Signaling Protocols and provisioned QoS resource management. |
| CoS | Class of Service. The type 4 tuple of a DOCSIS configuration file. |

| | |
|---------------|---|
| CSR | Customer Service Representative |
| DA | Directory Assistance |
| DE | Default. This is a DiffServ Per Hop Behavior. |
| DES | Data Encryption Standard |
| 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. |
| 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. |
| DSFID | Downstream Service Flow ID. See SFID |
| 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 |
| FEID | Financial Entity ID |
| FGD | Feature Group D signaling |
| FQDN | Fully Qualified Domain Name. Refer to IETF RFC 821 for details. |
| GC | Gate Controller |
| GTT | Global Title Translation |
| HFC | Hybrid Fiber/Coax (cable). An HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the head-end and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations. |
| 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 Telecommunications Union |
| ITU-T | International Telecommunications Union–Telecommunications 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. |
| lsb | Least significant bit |
| 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. |
| 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. |
| 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 PacketCable 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 head-end 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 and 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 numbers (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 Identifier |
| 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. |
| 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 |
| PHB | Per-Hop Behavior |
| 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 2138 and RFC 2139) 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 PacketCable. |
| 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. |
| RSVP | Resource Reservation Protocol |
| 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. Any 32-bit SFID must not conflict with a zero-extended 14-bit SID. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). USFIDs and DSFIDs 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 variant 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 |
| USFID | Upstream Service Flow ID. See SFID |
| 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

PacketCable MIBs are designed to provide necessary functionality defined in PacketCable specifications. The MIB design follows the same multi-phase schedule as the rest of PacketCable specifications. MIBs that are developed for PacketCable 1.0 support embedded-MTAs and provide definitions for call signaling and MTA device provisioning functions. Future PacketCable development phases will include other functional areas as well as requirements for other PacketCable components, which will be considered for MIB development. Table 1 lists PacketCable functional areas that are being considered for future PacketCable MIB definition.

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.

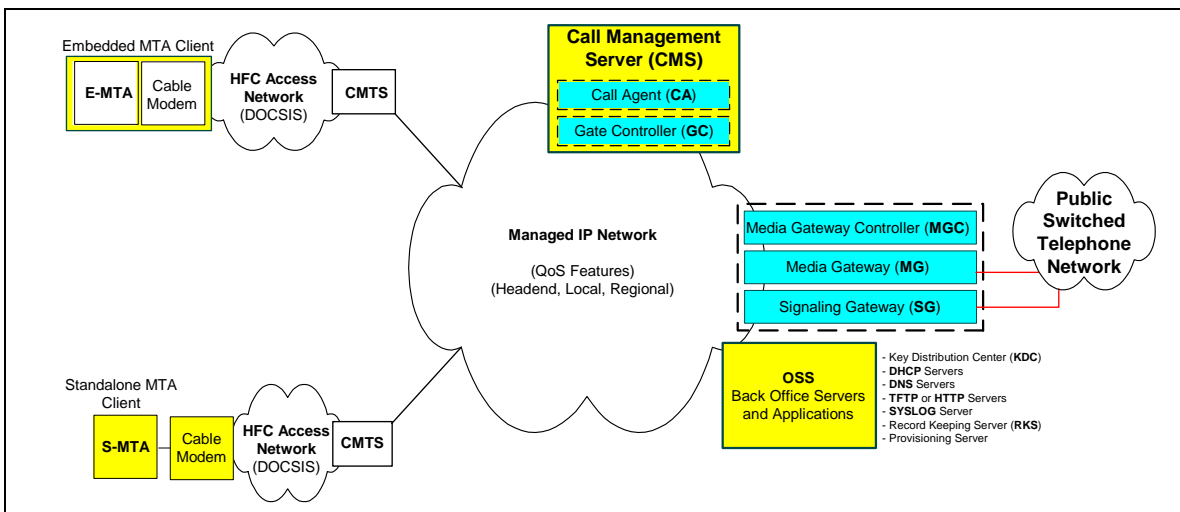


Figure 1. PacketCable Reference Architecture

5.2 General Requirements

The following requirements have been considered in design of PacketCable MIBs.

- PacketCable 1.0 devices must be compliant with DOCSIS 1.1; therefore PacketCable 1.0 devices MUST support DOCSIS 1.1 MIBs. The DOCSIS 1.1 MIB modules are [4], [5], and [6].
- Take a minimalist approach for design of the PacketCable MIB, i.e., if other MIBs define the same functions, then rely on these MIBs rather than create new ones.
- Organize MIBs to support both embedded and standalone MTA. Note that PacketCable 1.0 only requires embedded MTA support, but support of standalone MTA is foreseen in future PacketCable releases.
- Organize MIBs so as to allow functional partitioning of DOCSIS (high-speed data) and PacketCable (voice) features.
- DOCSIS 1.1 within PacketCable applications requires support of SNMPv3; therefore PacketCable MIBs MUST comply with SNMPv3.
- PacketCable MIBs MUST comply with SMIV2 and SNMPv2 as defined in RFC 2578.

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.

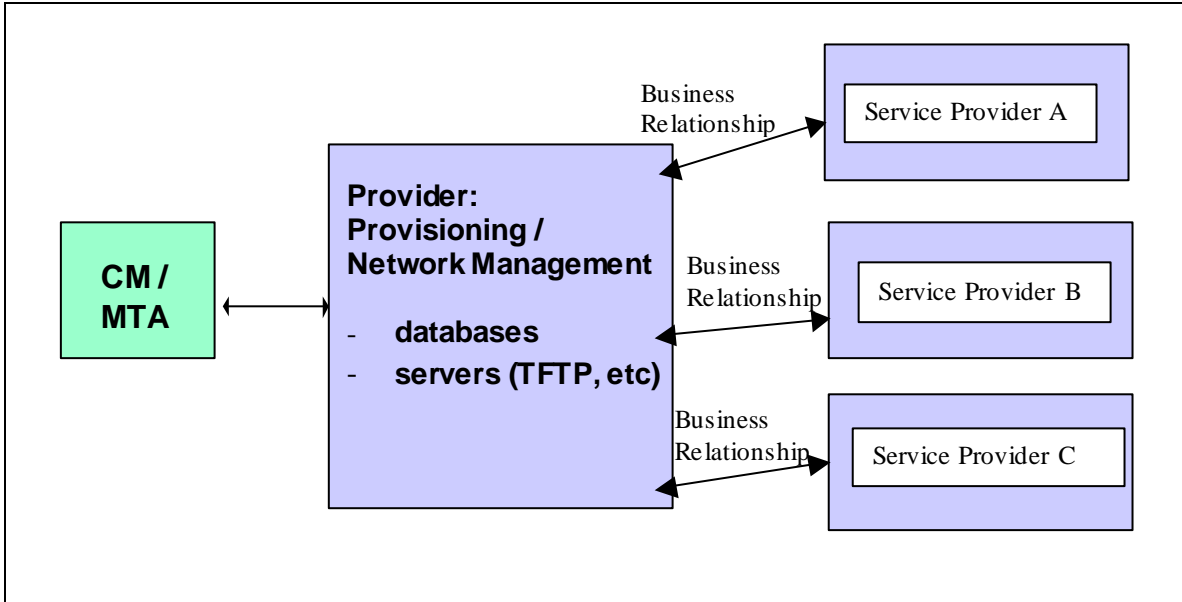


Figure 2. Partitioning of Management Domains

5.2.2 Support for Embedded and Standalone MTAs

The PacketCable MIBs includes 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 MIBs in common with DOCSIS. The Packetcable MIBs 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 [10].

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

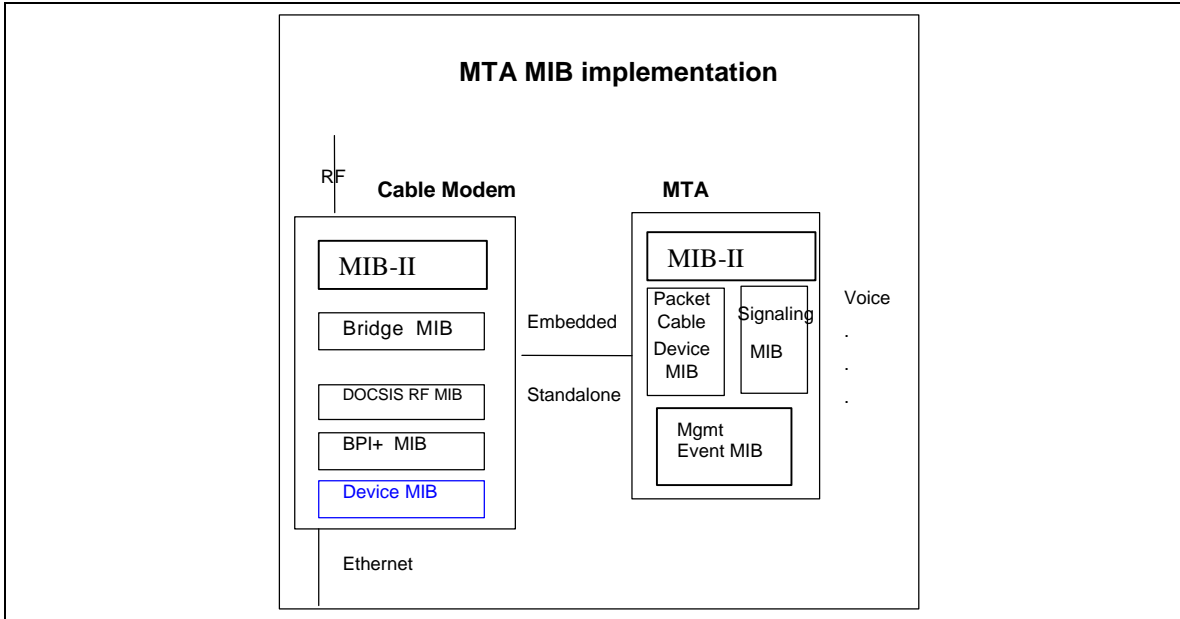


Figure 3. Embedded and Standalone MTA implementations

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 MIBs are used to define the content of the packets, the changes for SNMPv3 do not affect MIB design.

As of this writing the only requirements that imposed are that PacketCable MIBs MUST conform to SMIV2, which is described in RFC 2578 and 2579.

The following RFCs provide more information on SNMPv3.

- IETF RFC2571 An Architecture for Describing SNMP Management Framework
- IETF RFC2572 Message Processing and Dispatching for SNMP
- IETF RFC2573 SNMPv3 Applications
- IETF RFC2574 User Based Security Model for SNMPv3
- IETF RFC2575 View-Based Access Control Model (VACM) for SNMP

5.2.3.1 USM Requirements

For PacketCable 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 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 MIBs in the MTA, write access to PacketCable MIBS, and notifications as defined in the PacketCable MIBs

```

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 PacketCable defined MIBS. 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 MIBS, DOCSIS defined MIBS and vendor defined MIBS.

```

1.3.6.1                /* Full Internet MIB Tree*/

```

The NotifyView MUST consist of the MTA MIB and Management Event MIB. It MAY include vendor defined MIBS .

```

1.3.6.1.4.1.4491.2.2.1 /*MTA mib tree*/
1.3.6.1.4.1.4491.2.2.3 /*event mib tree*/

```

5.3 Functional Requirements

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

5.3.1 PacketCable Device Provisioning

The PacketCable 1.0 MIB should provide definitions for attributes that are required in the MTA device-provisioning flows. These attributes are documented in the PacketCable 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 PacketCable MIB 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 QoS (For consideration in future releases of PacketCable)

The PacketCable MIB should provide attributes for support of QoS on the MTA, as well as interoperate with QoS definitions of DOCSIS. Given that DOCSIS MIBs are including QoS attribute definitions, the PacketCable MIB will not be required to repeat these attributes. It might, however, be necessary to define

mechanisms for allocation of specific QoS in the PacketCable MIB in the specific case of voice communications services. Examples of these attributes are:

- Type of QoS protocol supported, D-QoS
- QoS authority
- QoS assignments:
- Provisioned bandwidth
- Admitted bandwidth
- Active bandwidth
- Service flow identifiers for each connection

5.3.4 Primary Line Requirements (For consideration in future releases of PacketCable)

The PacketCable MIB should provide attributes that are needed to satisfy high availability requirements of the voice communications service as defined in the PacketCable “primary line” specification. Examples of these attributes are power loss and network element failure.

5.3.5 Voice interfaces

PacketCable MIB 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.

5.3.6 Packet Voice Call Signaling

The PacketCable MIB should provide attributes that are needed for management of the packet voice call signaling protocol. As of this writing the only call signaling protocol that is being specified by PacketCable is NCS; however, work is also underway for DCS. Example 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

5.3.7 Packet Voice Transport (For consideration in future releases of PacketCable)

The PacketCable MIB should provide attributes that can be used to monitor and manage packet voice transport. As of this writing the RTP protocol is used for packet voice transport, and therefore the RTP MIB (IETF RFC 2959) can be used for management of the packet voice transport function of the MTA.

Given that the RTP MIB consists of attributes that relate to fault and performance data, it is not being considered for the 1.0 release of the PacketCable MIB.

5.3.8 Fault Management (For consideration in future releases of PacketCable)

The PacketCable MIB should provide attributes that can be used in management of network faults and failures. These attributes and functions related to these attributes are under consideration in the primary line focus group and will be included in the MIB in a later release. These attributes include:

- Standard alerts.
- Common fault messages (software upgrades, resets, link up/down).

- Prioritized alerts (0-7) for throttling and limiting and class.
- Possible “thin RMON” agent.
- Fault isolation.

5.3.9 Performance Management (For consideration in future releases of PacketCable)

The PacketCable MIB should provide attributes that can be used in monitoring of the performance of the network when used for voice communications. As of this writing no focus group is considering performance monitoring aspects of the PacketCable network. Examples of attributes that should be considered for performance monitoring are:

- Packet counts
- Call signaling status

5.3.10 Event Management

The PacketCable MIB should provide the means to define and distribute events generated by the MTA. It should provide the ability for vendors to define their own events as well as support 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. These means should include local log, syslog, SNMP traps and SNMP informs. Some means of event thresholding should be supported.

6 MIBS AVAILABLE IN A PACKETCABLE NETWORK

In designing the PacketCable MIB, it was necessary to consider other MIBs that are also present in the network and which can provide the required attributes and functions. This section describes the MIBs that can be present in the PacketCable MTA device, and which can be used for PacketCable management functions as needed.

The following table lists MIBs that are present in the PacketCable device. Note that the device can be a cable modem or an E-MTA or an S-MTA.

Table 2: Additional MIBs

| MIBs present in PacketCable Device |
|------------------------------------|
| DOCSIS 1.1 Cable Device MIB |
| DOCSIS 1.1 RF MIB |
| DOCSIS 1.1 QoS MIB |
| DOCSIS 1.1 BPI+ MIB |
| IF MIB |
| MIB II |
| Ethernet MIB |
| Bridge MIB |
| PacketCable Device MIB |
| SIGNALING MIB |
| Management Event MIB |

As mentioned before partitioning of voice and data services and support of both S-MTA and E-MTA has been requirements for design of the MIB. Figure 3 in the General Requirements section describes possible organizations of the MIB in order to meet these requirements. In doing so, the common MIB category was introduced which is basically a collection of MIBs, which can be present on both the cable modem as well as the MTA device.

6.1 DOCSIS 1.1 MIBs

PacketCable's embedded MTA is dependent on the following DOCSIS 1.1 MIBs. Please refer to the following documents for further information.

- *Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems*, IETF RFC 2669.
- *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces*, IETF RFC 2670.
- *Data Over Cable System Quality of Service Management Information Base (DOCSIS-QOS MIB)*, draft-ietf-ipcdn-qos-mib-04.txt.

6.2 IF MIB

This is the interfaces section of the MIB II (RFC 2863), and is needed for definitions of multiple interfaces in the MTA.

6.3 MIB II

RFC 1907, RFC 2011, and RFC 2131 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 PacketCable MTA device. The PacketCable 1.0 MIB 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 [7], section 4.2.1.

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

PacketCable ifTable MUST contain information about all PacketCable endpoints. IfIndex, in case of PacketCable 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 endpoint in an E-MTA MUST have a corresponding entry ("conceptual row") in the "ifTable" MIB Table.

The CableModem part of an embedded MTA MUST adhere to DOCSIS 1.1 and eDOCSIS [11] 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 MIBs 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.

Packetcable MTAs MUST implement [7], [8], [9], and [10]. PacketCable 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(3) |
| IfIndex | 1 |

6.4 Ethernet MIB

Definitions of Managed Objects for the Ethernet Like Interfaces. See RFC 2665.

6.5 Bridge MIB

Definitions of Managed Objects for Bridges. See RFC 1493.

6.6 PacketCable MTA SIGNALING MIB

The MTA SIGNALING MIB contains Call Signaling information for provisioning. The MTA SIGNALING MIB is derived as part of the PacketCable enterprise branch of MIB tree. Application for standard acceptance is being discussed. No other functionality other than MTA SIGNALING provisioning is defined at this time, although future releases of the MTA SIGNALING MIB may enhance the capabilities.

6.6.1 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.

6.6.2 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 [15]. This data only provides the means to provision network call signaling per endpoint.

6.7 PacketCable MTA Device MIB

The MTA Device MIB contains data for provisioning the MTA device and supporting the provisioned functions. The data is derived from the PacketCable provisioning specification [2], and the DOCSIS Cable Device MIB, RFC 2669. The MTA Device MIB is defined as part of the CableLabs enterprise branch of the MIB tree. Application for standard acceptance is being discussed. No other functionality other than device provisioning and support of provisioned data is defined at this time, although future releases of the MTA Device MIB may enhance the capabilities.

6.7.1 MTA Device MIB general configuration information

The MTA Device MIB contains general configuration information to provision the MTA on a device basis. These objects support provisioning required servers, security information, and non-type specific call signaling data.

6.7.2 MTA Device MIB Syslog Information

The MTA Device MIB contains syslog control information similar to DOCSIS. This is to maintain the syslog capability of the voice communication MTA separate from the DOCSIS CM syslog. As in DOCSIS, it supports a syslog server, local logging, and traps.

6.8 Event Management MIB

The Management Event MIB 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 MTA in a multi-vendor environment and provides a standard means to implement PacketCable specified events.

7 PACKETCABLE MIB IMPLEMENTATION

This section describes a reference implementation of the MIBs in a PacketCable device. Given that only E-MTA is supported for the PacketCable 1.0 release, we will only consider E-MTA type implementations here.

7.1 MTA components

Figure 4 below shows the components of a typical MTA.

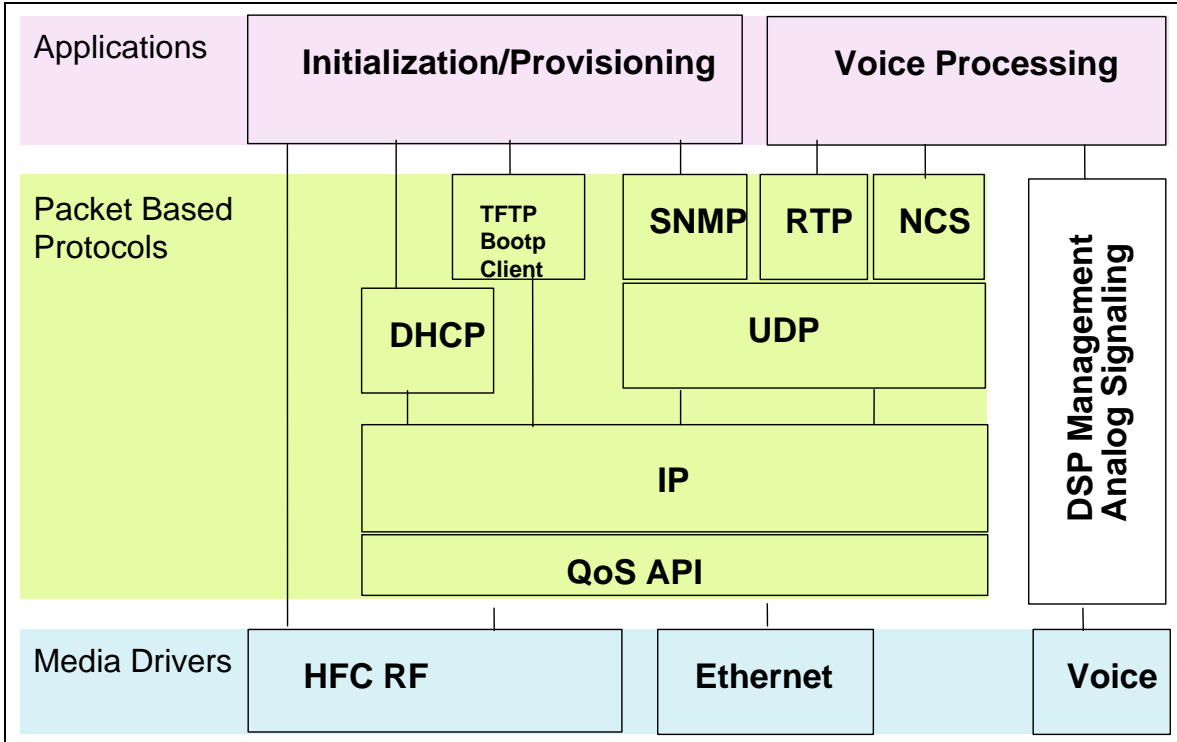


Figure 4. MTA Components

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. MIBs that are implemented in the MTA have to be organized so as to facilitate this separation. PacketCable 1.0 MIB specifies functions for the packet based protocol section of the MTA. As of this writing there are no analog voice MIBs specified for the MTA.

Note: Please refer to the security document [16] 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.

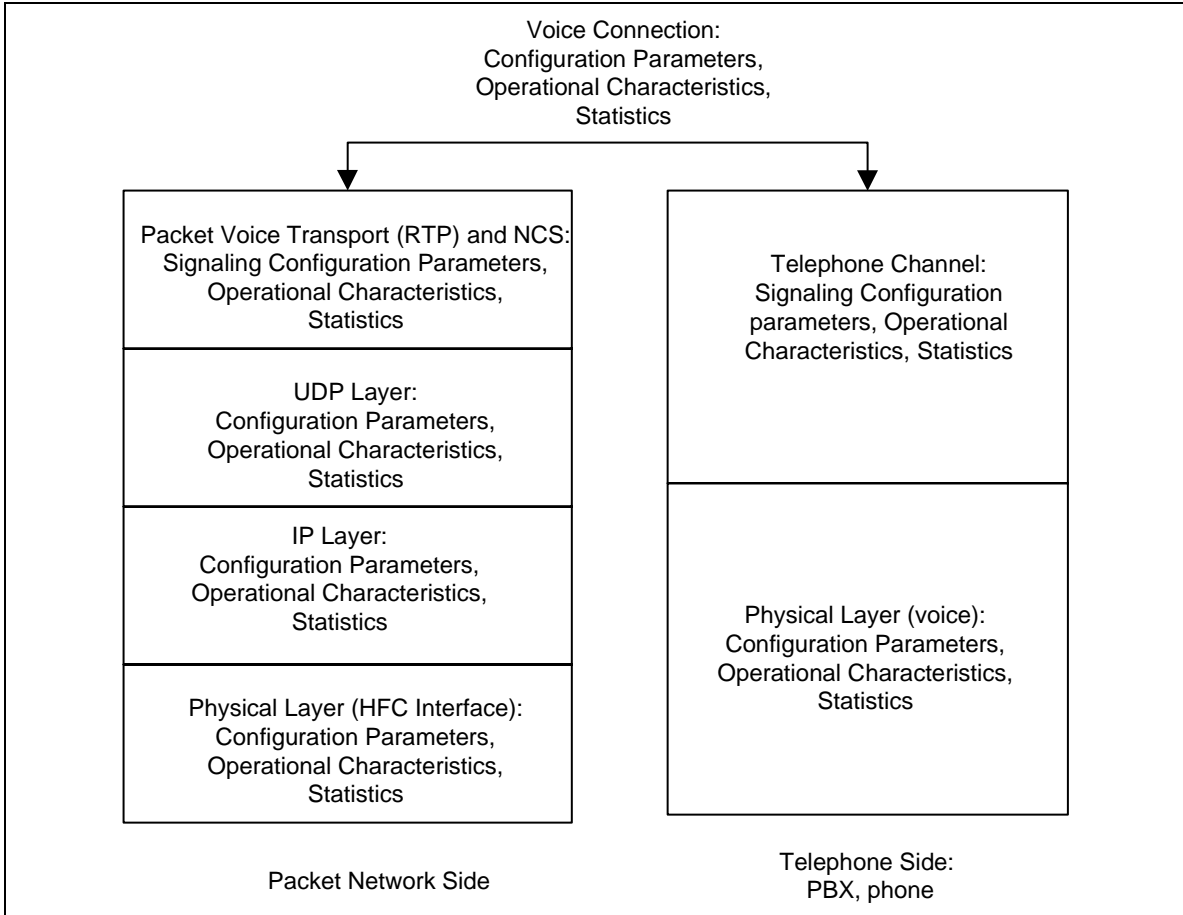


Figure 5. MIB Layering Model

In the context of voice communications, MIBs 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 PacketCable 1.0 does not specify any MIBs for the telephone side of the MTA.

Appendix A. CableLabs MIB Import Data

```

CLAB-DEF-MIB DEFINITIONS ::= BEGIN

IMPORTS

    MODULE-IDENTITY,
    enterprises

                                FROM SNMPv2-SMI;

cableLabs MODULE-IDENTITY

    LAST-UPDATED      "200211270000Z" --November 27, 2002
    ORGANIZATION      "Packet Cable OSS Group"
    CONTACT-INFO

        "Matt Osman
        Postal: Cable Television Laboratories, Inc.
              400 Centennial Parkway
              Louisville, Colorado 80027-1266
              U.S.A.
        Phone:  +1 303-661-9100
        Fax:    +1 303-661-9199
        E-mail: m.osman@cablelabs.com"

    DESCRIPTION

        "This MIB module supplies the basic management
        object categories for Cable Labs.

        Acknowledgements:
        Angela Lyda          -   Arris Interactive
        Roy Spitzer         -   Telogy Networks, Inc.
        Rick Vetter        -   Motorola
        Eugene Nechamkin   -   Broadcom Corp"

    ::= { enterprises 4491 }

clabFunction              OBJECT IDENTIFIER ::= { cableLabs 1 }
clabFuncMib2              OBJECT IDENTIFIER ::= { clabFunction 1 }
clabFuncProprietary      OBJECT IDENTIFIER ::= { clabFunction 2 }
clabProject               OBJECT IDENTIFIER ::= { cableLabs 2 }
clabProjDocsis            OBJECT IDENTIFIER ::= { clabProject 1 }
clabProjPacketCable      OBJECT IDENTIFIER ::= { clabProject 2 }
clabProjOpenCable        OBJECT IDENTIFIER ::= { clabProject 3 }
clabprojCableHome        OBJECT IDENTIFIER ::= { calbProject 4 }

```

```
-----  
--          Packet Cable branch definitions  
-----  
  
pktcMtaMib      OBJECT IDENTIFIER ::= { clabProjPacketCable 1 }  
pktcSigMib      OBJECT IDENTIFIER ::= { clabProjPacketCable 2 }  
pktcEventMib    OBJECT IDENTIFIER ::= { clabProjPacketCable 3 }  
pktcSmtaMib     OBJECT IDENTIFIER ::= { clabProjPacketCable 4 }  
--pktcSecurity  OBJECT IDENTIFIER ::= { clabProjPacketCable 5 }  
-- See PacketCable Security Specification PKT-SP-SEC_I02-001229  
-- for details.  
  
END
```

Appendix B. Bibliography Informative

- [13] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, SP-CMCI-I08-020830, August 30, 2002, Cable Television Laboratories, Inc.
- [14] Data-Over-Cable Service Interface Specifications, Cable Modem Termination System- Network Side Interface Specification, DOCSIS SP-CMTS-NSI-I01-960702, July 02, 1996, Cable Television Laboratories, Inc.
- [15] PacketCable Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I06-021127, November 27, 2002, Cable Television Laboratories, Inc., <http://www.PacketCable.com/>
- [16] PacketCable Security Specification, PKT-SP-SEC-I07-021127, November 27, 2002, Cable Television Laboratories, Inc., <http://www.PacketCable.com/>
- [17] PacketCable Distributed Call Signaling Specification, PKT-SP-DCS-D03-000428, Cable Television Laboratories, Inc., <ftp://ftp.cablelabs.com/pub/pkt-sp-dcs-d03-000428.pdf>
- [18] PacketCable Dynamic Quality of Service Specification, PKT-SP-DQOS-I05-021127, November 27, 2002, Cable Television Laboratories, Inc., <http://www.PacketCable.com/>
- [19] IETF RFC 2572 Message Processing and Dispatching for SNMP
- [20] IETF RFC 2573 SNMPv3 Applications
- [21] IETF RFC 2574 User Based Security Model for SNMPv3
- [22] IETF RFC 2575 View-Based Access Control Model (VACM) for SNMP
- [23] IETF RFC 2578 Structure of SMIV2
- [24] IETF RFC 2579 Textual Conventions for SMIV2
- [25] Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification SP-OSSIV1.1-I06-020830, August 30, 2002, Cable Television Laboratories, Inc.
- [26] IETF RFC 1643 Definitions of Managed Objects for the Ethernet Like Interfaces
- [27] IETF RFC 1493 Definitions of Managed Objects for Bridges
- [28] IETF RFC 2233 The Interfaces Group MIB Using SMIV2
- [29] IETF RFC 1907 MIB for SNMPv2
- [30] IETF RFC 2011 SNMPv2 MIB for the Internet Protocol Using SMIV2
- [31] IETF RFC 2013 SNMPv2 MIB for the User Datagram Protocol Using SMIV2

Appendix C. 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),
Rick Morris (Arris),
Klaus Hermanns (Cisco),
Eugene Nechamkin (BroadCom Corp.),
Rick Vetter (Motorola/GI),
Roy Spitzer (Telogy/TI)

Matt Osman, CableLabs

Appendix D. Revisions

Engineering Change Numbers

The following Engineering Change Notices have been incorporated into PKT-SP-MIBS-I03-020116:

| ECN | Date Ratified | Summary |
|---------------|---------------|--|
| mib-n-01023 | 03/26/01 | It is not clear how the manager can determine which vendor proprietary MIBs must be used in managing a particular MTA. |
| mib-n-01164v2 | 10/22/01 | Spec clarification on the usage of the “ifTable” and “ifIndex” in E-MTA. |
| mib-n-01189 | 12/10/01 | Add requirements for VACM and USM for MTA |

The following Engineering Change Notices have been incorporated into PKT-SP-MIBS-I04-021018:

| ECN | Date Ratified | Summary |
|--------------|---------------|---|
| prov-n-02005 | 8/5/02 | Delete entries from VACM tables. |
| mibs-n-02030 | 8/5/02 | Align the MTA's MIB II sysDescr object format with the DOCSIS MIBII sysDescr format |

The following Engineering Change Notices have been incorporated into PKT-SP-MIBS-I05-021127.

| ECN | Date Ratified | Summary |
|--------------|---------------|--|
| mibs-n-02180 | 11/18/02 | The ifAdminStatus MIB, 1.3.6.1.2.1.2.2.1.7, is currently set to ReadOnlyView from the MTA side and must be set to FullAccessView. |
| mibs-02207 | 11/20/02 | Aligns the PacketCable MIB requirements with the proposed CableLabs' general MIB framework for devices which are embedded with a DOCSIS Cable Modem. |