Superseded

PacketCable™ MIBs Framework Specification

PKT-SP-MIBS-I01-991201

Interim

Notice

Document Status Sheet

Document Control Number:	PKT-SP-MIBS-I01-991201			
Document Title:	PacketCable™ MIBs Framework Specification			
Revision History:	I01-991201: release			
Date:	December 1, 1999			
Status:	~~Work in Progress~~	~~Draft~~	Interim	~~Released~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ 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.
Interim	A document which has undergone rigorous Member and vendor review, suitable for use by vendors to design in conformance to and for field testing. For purposes of the “Contribution and License Agreement for Intellectual Property" which grants licenses to the intellectual property contained in the PacketCable Specification, an “Interim Specification" is a "Published” Specification.
Released	A stable document, reviewed, tested and validated, suitable to enable cross-vendor interoperability.

Contents

Figures

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 functions and how the requirements are supported in the MIB. It is intended to support and complement the actual MIB documents where it is deemed necessary.

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 should be recalled 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, and that these differences may be significant for legal/regulatory purposes.

1.2 PacketCable Reference Architecture

The conceptual diagram for the PacketCable architecture is shown in Figure 1. Please refer to the architecture document [7] for more detailed information concerning the PacketCable architecture.

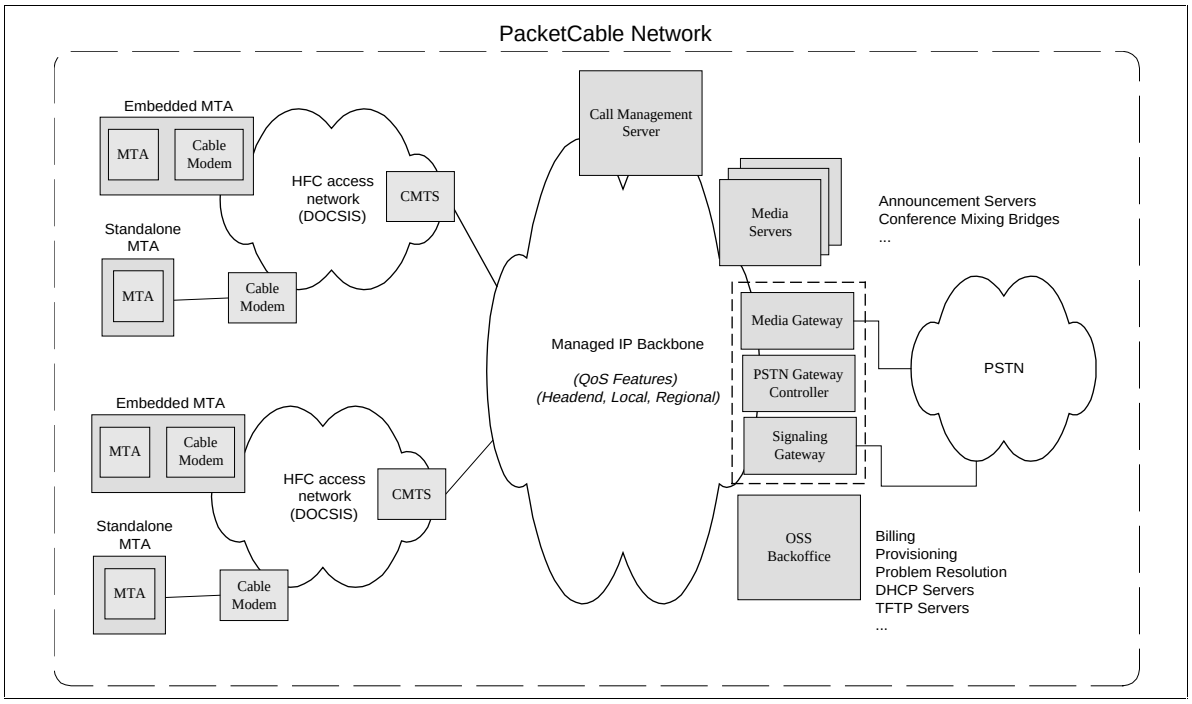

Figure 1. PacketCable Reference Architecture

1.3 Scope

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 NCS 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.

Table 1 : Functional MIB Areas

PacketCable Specification	Phase	MIB development
DCS Signaling	Future	TBD
NCS Signaling	1.0/Future	MTA NCS MIB Telephony config file CMS NCS MIB (Future)
Device Provisioning	1.0	MTA Device MIB Telephony config file
Primary Line	Future	TBD
Packet Voice transport	Future	TBD

PacketCable Specification	Phase	MIB development
Codec	1.0/Future	MTA NCS MIB
Security	1.0	MTA Device MIB Telephony config file
Performance	Future	Incorporation of RTP MIB Additions to NCS MIB
D-QoS	Future	TBD
LAESS	Future	TBD

1.4 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 weighted 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 included the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

1.5 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 (revision 7) MIBs. The DOCSIS 1.1 MIB modules are:
    - Cable Device MIB (revision 7)
    - Radio Frequency MIB (revision 7)
    - QoS MIB (under development)
- 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 stand-alone 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 to SNMPv3.
- PacketCable MIBs MUST comply to SMIv2 and SNMPv2 as defined in RFC 2578.

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

1.5.1 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.

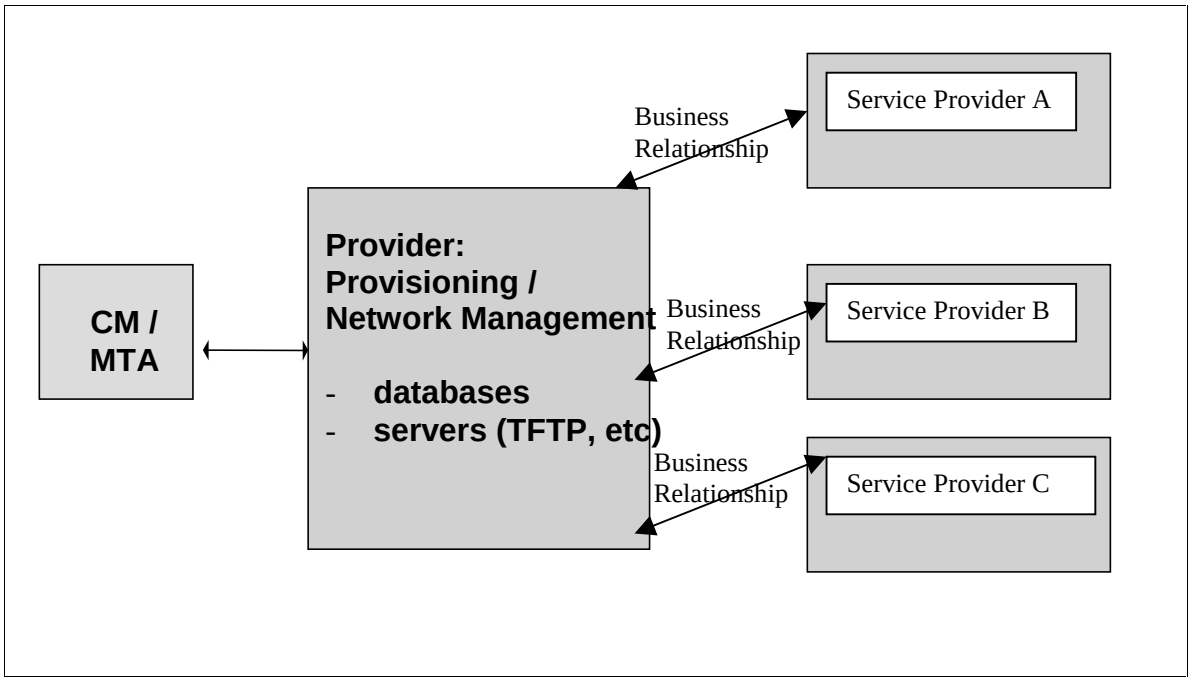

Figure 2. Partitioning of Management Domains

1.5.2 Support for Embedded and Standalone MTAs

The PacketCable MIBs will provide features for both embedded and standalone MTAs. Standalone MTAs are not required to include any DOCSIS related functions, The PacketCable MIBs, therefore should be independent of DOCSIS and able to provide management support for voice communications functionalities using a standalone MTA device that does not have DOCSIS as a base. Although definitions and design of the standalone MTA is not part of PacketCable 1.0, the MIBs have been designed with the understanding that they will be used in S-MTA implementations in the future.

Figure 3 describes possible MIB implementations for embedded and standalone MTAs. Note that the S-MTA definitions are TBD.

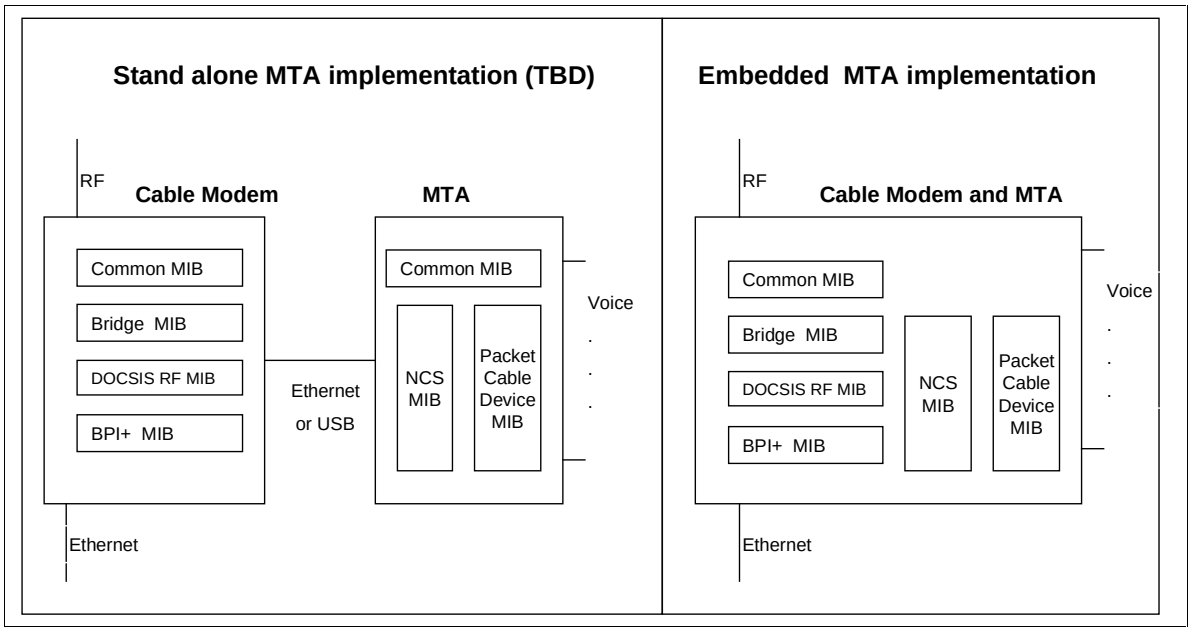

Figure 3. Embedded and Standalone MTA implementations

In this figure, the MIBs are divided into categories that can be placed into both E-MTA and S-MTA. The box that is labeled as "common MIB" represents a set of MIBs that has to be present on any device. An example of a common MIB is the interfaces group of MIB II.

1.5.3 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 effect 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.

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

1.6 Functional Requirements

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

1.6.1 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 [9] 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.

1.6.2 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.

1.6.3 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

1.6.4 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.

1.6.5 Voice interfaces (For consideration in future releases of PacketCable)

The PacketCable MIB should provide attributes that can be used to manage voice ports on the MTA. As of this writing these ports are not being specified by any PacketCable focus group. The PacketCable architecture document only mentions support of the analog 2500 phone. A complete definition of the characteristics of

these ports can be scheduled for future PacketCable work. Examples of voice port attributes that can be included in the MIB include:

- Physical port description
- Analog – 2500 (POTS) phone, E&M
- Digital – ISDN
- Signaling protocols used on this interface
- Dialtone delay
- Minimum call setup latency time

1.6.6 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

1.6.7 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 (IETTF draft-ietf-avt-rtp-mib-05.txt) 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.

1.6.8 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.

1.6.9 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

2 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
NCS 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.

2.1 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," draft-ietf-ipcdn-cable-device-mib-08.txt.
- "Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces," draft-ietf-ipcdn-rf-interface-mib-08.txt.
- "Data Over Cable System Quality of Service Management Information Base (DOCSIS-QOS MIB)," draft-ietf-ipcdn-qos-mib-01.txt.

2.2 IF MIB

This is the interfaces section of the MIB II (RFC 2233), and is needed for definitions of multiple interfaces in the MTA.

2.3 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 internets. 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.

The interfaces table provides mechanism for identification and independent management of the interfaces in the device.

The IP object group provides information that is relevant to the IP protocol.

The transmission group provides a mechanism for other MIBs that are related to the underlying media for that interface to be hooked in to the MIB tree.

2.4 Ethernet MIB

Definitions of Managed Objects for the Ethernet Like Interfaces. See RFC 1643.

2.5 Bridge MIB

Definitions of Managed Objects for Bridges. See RFC 1493.

2.6 PacketCable MTA NCS MIB

The MTA NCS MIB contains Network Call Signaling information for provisioning. The data is derived from the PacketCable NCS specification. The MTA NCS 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 MTA NCS provisioning is defined at this time, although future releases of the MTA NCS MIB may enhance the capabilities.

2.6.1 MTA NCS MIB general configuration information

The MTA NCS MIB contains general configuration information that applies to network call signaling on a device basis. This information is also found in the configuration file defined in the PacketCable NCS specification [4].

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

2.6.2 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 [4]. This data only provides the means to provision network call signaling per endpoint.

2.7 PacketCable MTA Device MIB

The MTA Device MIB contains data for provisioning the MTA device and supporting the provisioned functions, specifically syslog. The data is derived from the PacketCable provisioning specification [9], and the DOCSIS Cable Device MIB, draft-ietf-ipcdn-cable-device-mib-08.txt. 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.

2.7.1 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.

2.7.2 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.

3 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.

3.1 MTA components

Figure 4 below shows the components of a typical MTA.

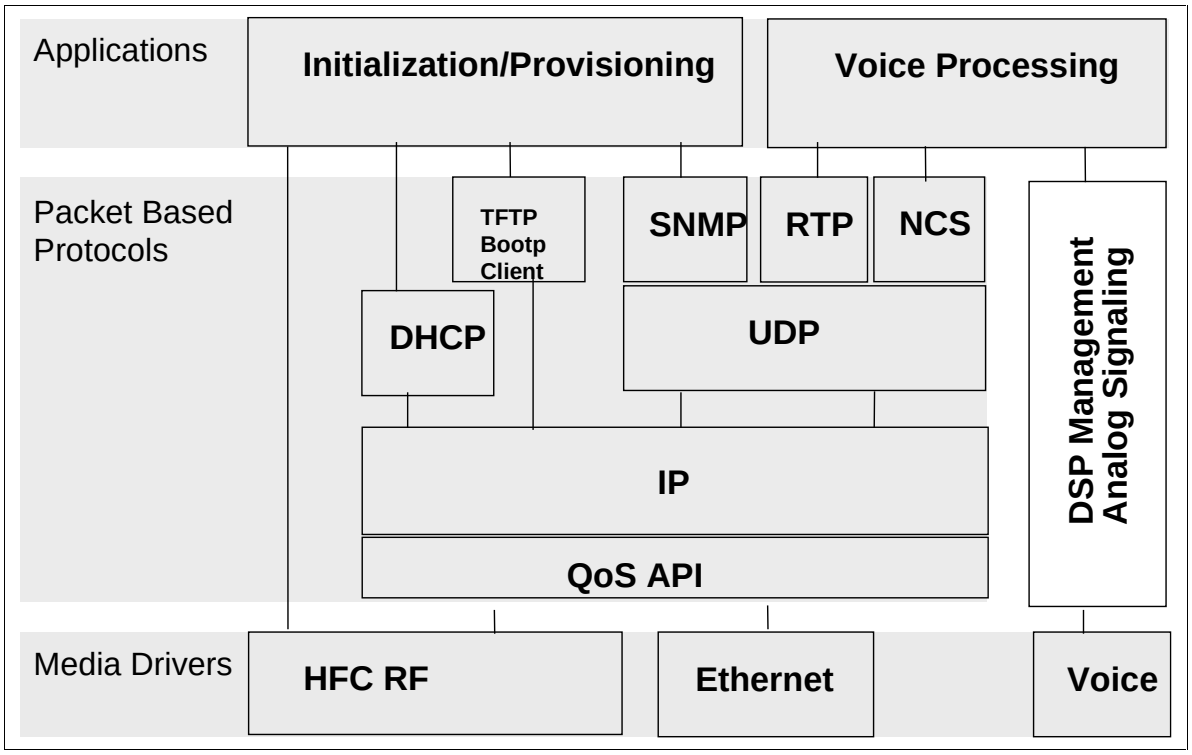

Figure 4. MTA Components

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.

3.2 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.

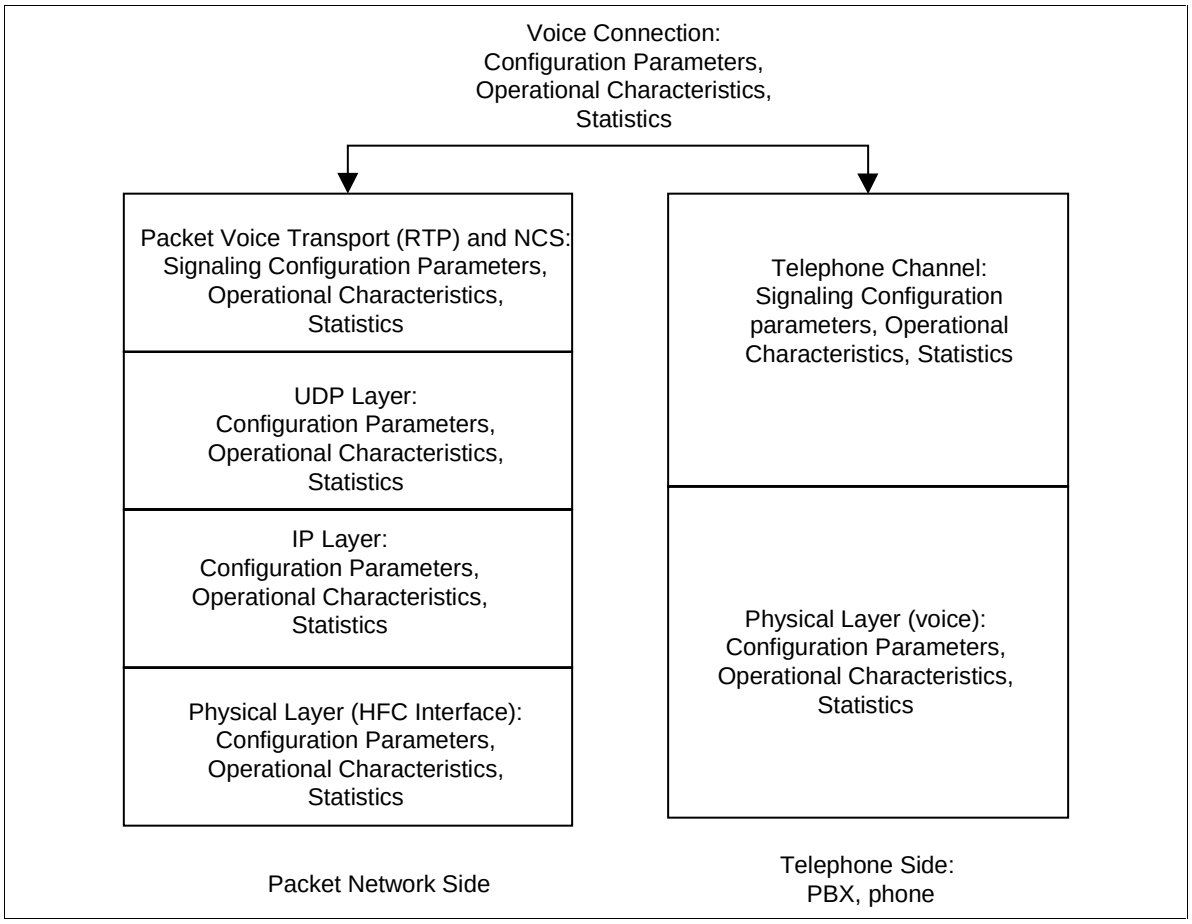

Figure 5. MIB Layering Model

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

The CableLabs MIB containing import data required for import by PacketCable NCS MIB and MTA MIB is shown below.

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
        enterprises
    FROM SNMPv2-SMI;
        cableLabs MODULE-IDENTITY
    LAST-UPDATED    "9910280000Z"  -- October 28, 1999
    ORGANIZATION    "Packet Cable OSS Group"
    CONTACT-INFO
        "Maria Stachelek
         Cable Labs
           E-mail: maria@cablelabs.com"
    DESCRIPTION
        "This MIB module supplies the basic management
         object categories for Cable Labs.  "
    ::= { 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 }
END
```

Appendix B. 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 Angela Lyda and Rick Morris (Arris), Azita Kia, Klaus Hermanns and Azlina Palmer (Cisco), Babu Prabesh (Com21), Rick Vetter (GI), Roger Loots (Lucent), and Roy Spitzer (Telogy) for their contribution to this document.

Maria Stachelek, CableLabs

Appendix C. Glossary and Acronyms

AAA	Authentication, Authorization and Accounting
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.
AF	Assured Forwarding. A Diffserv Per Hop Behavior.
AH	Authentication header is an IPSec security protocol that provides message integrity for complete IP packets, including the IP header.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access".
Announcement Server	An announcement server plays informational announcements in PacketCable network. Announcements are needed for communications that do not complete and to provide enhanced information services to the user.
AMA	Automated Message Accounting., a standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies)
Asymmetric Key	An encryption key or a decryption key used in a public key cryptography, where encryption and decryption keys are always distinct.
AT	Access Tandem
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
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 who claims to have given the information.
Authorization	The act of giving access to a service or device if one has the permission to have the access.
BAF	Bellcore AMA Format, another way of saying AMA
BPI+	Baseline Privacy Interface Plus is the security portion of the DOCSIS 1.1 standard which runs on the MAC layer.
CBC	Cipher block chaining mode is 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.
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. In this specification "Call Agent" is part of the CMS that maintains the communication state, and controls the line side of the communication.

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
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.
CIR	Committed Information Rate.
Cleartext	The original (unencrypted) state of a message or data.
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.
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.
Codec	COder-DECoder
Confidentiality	A way to ensure that information is not disclosed to any one other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
COPS	Common Open Policy Service Protocol is 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 1.0 configuration file.
CSR	Customer Service Representative
Cryptoanalysis	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.
DA	Directory Assistance
DE	Default. A Diffserv Per Hop Behavior.
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
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default - Network Provider DHCP Server

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
DNS	Domain Name Server
Downstream	The direction from the head-end toward the subscriber location.
DSCP	Diffserv Code Point. A field in every IP packet which 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. See Appendix A.
DOCSIS	Data Over Cable System Interface Specification.
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, i.e. assigned on the fly for each communication depending on the QoS requested
DTMF	Dual-tone Multi Frequency (tones)
EF	Expedited Forwarding. A Diffserv Per Hop Behavior.
E-MTA	Embedded MTA – a single node which contains both an MTA and a cable modem.
Encipherment	A method used to translate information in plaintext into ciphertext.
Encryption	A method used to translate information in plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or MCU
EO	End Office
Errored Second	Any 1-sec interval containing at least one bit error.
ESP	IPSec Encapsulation Security Payload protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute
Event Message	Message capturing a single portion of a connection
FGD	Feature Group D signaling
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated"
Flow [IP Flow]	A unidirectional sequence of packets identified by ISO 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.
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow"). A unidirectional sequence of packets associated with a SID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 821 for details.
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 tot he edge of the PacketCable network.

H.323	An ISO standard for transmitting and controlling audio and video information. The H.323 standard requires the use of the H.225/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.
HFC	Hybrid Fiber/Coax(ial [cable]), 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.
H.GCP	A protocol for media gateway control being developed by ITU.
HMAC	Hashed Message Authentication Code – a message authentication algorithm, based on either SHA-1 or MD5 hash and defined in RFC 2104.
HTTP	Hyper Text 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 in the Internet.
IKE	Internet Key Exchange is 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, which requires digital certificates for authentication.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access Transport Area
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
ISUP	ISDN User Part is a protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ISTP	Internet Signaling Transport Protocol
ISTP – User	Any element, node, or software process that uses the ISTP stack for signaling communications.
ITU	International Telecommunication Union
IVR	Interactive Voice Response System
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.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of 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.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
LATA	Local Access and Transport Area
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
LD	Long Distance
LIDB	Line Information Data Base, containing information on customers required for real-time access such as calling card personal identification numbers (PINs) for real-time validation
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
LLC	Logical Link Control, used here to mean the Ethernet Packet header and optional 802.1P tag which may encapsulate an IP packet. A sublayer of the Data Link Layer.
LNP	Local Number Portability. Allows a customer to retain the same number when switching from one local service provider to another.
LSSGR	LATA Switching Systems Generic Requirements
MAC	Message Authentication Code - a fixed length data item that is sent together with a message to ensure integrity, also known as a MIC.
MAC	Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
MC	Multipoint Controller
MD5	Message Digest 5 - a one-way hash algorithm which maps variable length plaintext into fixed length (16 byte) ciphertext.
MDCP	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	The media gateway provides the bearer circuit interfaces to the PSTN and transcodes the media stream.
MGC	An Media Gateway Controller is the overall controller function of the PSTN gateway. It receives, controls and mediates call signaling information between the PacketCable and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow on to SGCP.
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 MAC.
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media

	streams of multiple connections.
MSO	Multi-System Operator, a cable company that operates many head-end locations in several cities.
MSU	Message Signal Unit
MTA	Media 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 is a set of two protocols (MTP 2, 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; the layer that provides services to establish a path between open systems.
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.
NCS	Network Call Signaling
Nonce	A random value used only once which 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.
NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP)
NTP	Network Time Protocol, an internet standard used for synchronizing clocks of elements distributed on an IP network
NTSC	National Television Standards Committee which defines the analog color television, broadcast standard used today in North America.
Off-Net Call	A communication connecting a PacketCable subscriber out to a user on the PSTN
On-Net Call	A communication placed by one customer to another customer entirely on the PacketCable Network
One-way Hash	A hash function that has an insignificant number of collisions upon output.
OSP	Operator Service Provider
OSS-D	OSS Default – Network Provider Provisioning Server
OSS	Operations Systems Support. The back office software used for configuration, performance, fault, accounting and security management.

PAL	Phase Alternate Line – the European color television format which evolved from the American NTSC standard.
PDU	Protocol Data Unit
PKCS	Public Key Cryptography Standards, published by RSA Data Security Inc. Describes 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	The extension to the Kerberos protocol that provides a method for using public key cryptography during initial authentication.
PHS	Payload Header Suppression, a DOCSIS technique for compressing the Ethernet, IP and UDP headers of RTP packets.
Plaintext	The original (unencrypted) state of a message or data.
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 then 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 there by eliminating a host from having to support the services themselves.
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.
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 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 users private key is kept secret and is the only key which can decrypt messages sent encrypted by the users public key.
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.
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service, guarantees network bandwidth and availability for applications.
RADIUS	Remote Access Dial-In User Service, an internet protocol (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	A variable key length stream cipher offered in the ciphersuite, 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	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
RKS	Record Keeping Server, the device which collects and correlates the various Event Messages
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 that it generated with the corresponding root private key.
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 Protocol, a protocol defined in RFC 1889 for encapsulating encoded voice and video streams.
S-MTA	Standalone MTA – a single node which contains an MTA and a non DOCSIS MAC (e.g. ethernet).
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 BPI+ security protocol, part of the DOCSIS 1.1 specification.
SCCP	The Signaling Connection Control Part is a protocol within the SS7 suite of protocols that provides two functions in addition to those that are provided within MTP. The first is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	A Service Control Point is a Signaling Point within the SS7 network, identifiable by a Destination Point Code, that provides database services to the network.
SCTP	Simple Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information that is delivered as a unit between peer service access points.
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.
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 variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1 - a one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed by using encryption.
SIP	Session Initiation Protocol is an application layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants.
SIP+	Session Initiation Protocol Plus is an extension to SIP.
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SPI	Security Parameters Index - a field in the IPSEC header that along with the destination IP address provides a unique number for each SA.
SS7	Signaling System Number 7. SS7 is an architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Signal 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. An STP is a node within an SS7 network that routes signaling messages based on their destination address. It is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and 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.

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 used to grant Kerberos tickets.
TGW	Telephony Gateway
TIPHON	Telecommunications & Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value 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.
Transit Delays	The time difference between the instant at which the first bit of a 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 which carries user media content and may carry voice signaling (MF, R2, etc.).
TSG	Trunk Subgroup
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.
UDP	User Datagram Protocol, a connectionless protocol built upon Internet Protocol (IP).
Upstream	The direction from the subscriber location toward the head-end.
VAD	Voice Activity Detection
VBR	Variable bit-rate
VoIP	Voice over IP
WBEM	Web-Based Enterprise Management (WBEM) is the umbrella under which the DMTF (Desktop Management Task Force) will fit its current and future specifications. The goal of the WBEM initiative is to further management standards using Internet technology in a manner that provides for interoperable management of the Enterprise. There is one DMTF standard today within WBEM and that is CIM (Common Information Model). WBEM compliance means adhering to the CIM. See www.dmtf.org
X.509 certificate	a public key certificate specification developed as part of the ITU-T X.500 standards directory

Appendix D. References and Bibliography

[1]. Cable Modem to Customer Premise Equipment Interface Specification, CMCI, DOCSIS SP-CMCI-I02-980317, Cable Television Laboratories, Inc.

[2]. Cable Modem Termination System—Network Side Interface Specification, CMTS-NSI", DOCSIS SP-CMTS-NSII01-XXXXXX, Cable Television Laboratories, Inc.

[3]. PacketCable Product Specification, Cable Television Laboratories Inc., November 25, 1998.

[4]. PacketCable Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I02-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[5]. PacketCable Security Specification, PKT-SP-SEC-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[6]. PacketCable Distributed Call Signaling Specification, PKT-SP-DCS-D02-991007, October 10,1999, Cable Television Laboratories, Inc.

[7]. PacketCable Architecture Framework, PKT-TR-ARCH-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[8]. PacketCable Dynamic Quality of Service Specification, PKT-SP-DQOS-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[9]. PacketCable MTA Device Provisioning Specification, PKT-SP-PROV-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

[10]. RFC 2571 An Architecture for Describing SNMP Management Framework

[11]. RFC 2572 Message Processing and Dispatching for SNMP

[12]. RFC 2573 SNMPv3 Applications

[13]. RFC 2574 User Based Security Model for SNMPv3

[14]. RFC 2575 View-Based Access Control Model (VACM) for SNMP

[15]. RFC 2578 Structure of SMIv2

[16]. RFC 2579 Textual Conventions for SMIv2

[17]. "MCNS Data Over Cable Services Operations Support System Interface Specification SP-OSSII01-970403", MCNS, March 1997.

[18]. RFC 1643 Definitions of Managed Objects for the Ethernet Like Interfaces

[19]. RFC 1493 Definitions of Managed Objects for Bridges

[20]. RFC 2233 The Interfaces Group MIB Using SMIv2

[21]. RFC 1907 MIB for SNMPv2

[22]. RFC 2011 SNMPv2 MIB for the Internet Protocol Using SMIv2

[23]. RFC 2013 SNMPv2 MIB for the User Datagram Protocol Using SMIv2

Appendix E. Revisions

Engineering Change Numbers

ECN	Date Ratified	Summary