

# **Superseded by**

# **PacketCable 1.5**

PacketCable™ Management Event  
Mechanism Specification

# **Specs**

**PKT-SP-MEM-I01-001128**

**Interim**

## **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 2000 Cable Television Laboratories, Inc.

All rights reserved.

Document Status Sheet

**Superseded by**

**PacketCable 1.5**

**Specs**

<b>Document Control Number:</b> PKT-SP-MEM-I01-001128			
<b>Document Title:</b> PacketCable™ Management Event Mechanism Specification			
<b>Revision History:</b> I01-001128: release			
<b>Date:</b> November 28, 2000			
<b>Status:</b>	Work in Progress	Draft	Released
<b>Distribution Restrictions:</b>			
Author Only	<del>CL/Member</del>	<del>CL/Member/Vendor</del>	Public

**Key to Document Status Codes:**

- Work in Progress** An incomplete document designed to guide discussion and generate feedback that 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

<b>1 INTRODUCTION</b> .....	<b>1</b>
1.1 Purpose .....	1
1.2 Scope.....	1
1.3 Organization of Document .....	1
<b>2 REFERENCES</b> .....	<b>3</b>
<b>3 TERMS AND DEFINITIONS</b> .....	<b>4</b>
<b>4 ABBREVIATIONS AND ACRONYMS</b> .....	<b>5</b>
<b>5 BACKGROUND</b> .....	<b>12</b>
<b>6 PACKETCABLE 1.1 MANAGEMENT EVENT MECHANISM FUNCTIONAL REQUIREMENTS</b> .....	<b>13</b>
<b>7 MANAGEMENT EVENT REPORTING MECHANISM</b> .....	<b>15</b>
7.1 PacketCable Management Event Format .....	15
7.2 PacketCable Management Event Access Method .....	15
7.3 Management Event ID.....	16
7.4 Management Event Severities.....	16
7.4.1 Changing Default Event Severities .....	16
7.5 Programmable Events .....	17
7.5.1 Description .....	17
7.5.2 Default Display String Change Mechanism .....	17
7.6 Notification Mechanism.....	17
7.7 Local Log of Events.....	17
7.8 Event Throttling .....	17
7.9 Severity and Priority Definition.....	18
<b>8 PACKETCABLE MANAGEMENT EVENT DATA TEMPLATE</b> .....	<b>20</b>
<b>APPENDIX A. ACKNOWLEDGEMENTS</b> .....	<b>21</b>
<b>APPENDIX B. REVISIONS</b> .....	<b>22</b>



# Superseded by

## 1 INTRODUCTION

### 1.1 Purpose

This specification defines the Management Event Mechanism that PacketCable™ elements can use to report asynchronous events that indicate malfunction situations and notification about important information.

Events are defined in this specification as conditions requiring the reporting of information to management systems and/or local log.

A goal of PacketCable is to maintain consistency with the DOCSIS™ event reporting mechanism[13]. This PacketCable specification is being issued to facilitate design and field-testing leading to the early manufacturability and interoperability of conforming hardware and software by multiple vendors.

### 1.2 Scope

This specification is one of three documents that together define a framework for reporting Management Events in the PacketCable architecture.

This specification defines the general event reporting mechanism and framework. The mechanism consists of a set of protocols and interfaces that can be used by individual elements and components in the PacketCable architecture. This document defines how the SNMPv3 transport protocol, SYSLOG, local log, and the PacketCable MGMTEVENT MIB are used to carry management event information to an event management system.

This management event mechanism is further defined and supported by two other PacketCable documents: the Management Event Mechanism MIB and the Event-ID Technical Report.

1. PKT-SP-MIB-MGMTEVENT. This specification defines the associated Management Event Mechanism MIB that can be implemented on PacketCable elements such as the MTA, CMS, and others.
2. PKT-TR-MEMEVENT-ID. This technical report contains a summary of all PacketCable-defined Events. This document contains the PacketCable assigned Event ID for each PacketCable-defined event. Note that the specific descriptions and definitions of each PacketCable-defined event is contained in the individual PacketCable specifications.

### 1.3 Organization of Document

This document is structured as follows:

- Section 5 – Background information including a description of possible back office Network Management System (NMS) configurations and a brief description of supported PacketCable reporting mechanisms.
- Section 6 – Management Event Mechanism Functional Requirements.

- Section 7 – Detailed description of the Management Event Mechanism including definition of the event format, event access method, event IDs, event severities, programmable events, notification mechanism, local log of events, event throttling, and definition of severities and priorities.
- Section 8 – Example template for the management data.

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.

## 2 REFERENCES

- [1] “PacketCable 1.0 Architecture Framework Technical Report,” PKT-TR-ARCH-I01-001201, December 1, 1999, CableLabs Television Laboratories, Inc., <http://www.PacketCable.com/> (Informative Reference)
- [2] “PacketCable OSS Overview,” PKT-TR-OSSI-V02-991201, December 01, 1999, Cable Television Laboratories, Inc., <http://www.PacketCable.com/> (Normative Reference)
- [3] “PacketCable MTA MIB Specification,” PKT-SP-MIB-MTA-I01-991201, December 01, 1999. Cable Television Laboratories, Inc., <http://www/ PacketCable.com/> (Informative Reference)
- [4] “PacketCable MIB Framework Specification,” PKT-SP-MIB-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., <http://www.PacketCable.com/> (Informative Reference)
- [5] “PacketCable Event Messages Specification,” PKT-SP-EM-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., <http://www.PacketCable.com/> (Normative Reference)
- [6] “PacketCable MTA Device Provisioning Specification,” PKT-SP-PROV-I01-991201, December 01, 1999, Cable Television Laboratories, Inc., <http://www.PacketCable.com/> (Normative Reference)
- [7] “PacketCable Management Event ID Definitions,” PKT-TR-MGMTEVENT-ID-V01-000729, September 29,2000, Cable Television Laboratories, Inc., <http://www.PacketCable.com/> (Normative Reference)
- [8] “DOCSIS RF Interface MIB,” IETF RFC 2670 (Informative Reference)
- [9] “SNMP Applications,” IETF RFC 2573, <http://www.IETF.org/> (Informative Reference)
- [10] “Network Maintenance: Alarm and Control for Network Elements,” Bellcore GR-474 (Normative Reference)
- [11] “Generic Network Information Model,” ITU-T M.3100 (Normative Reference)
- [12] ”Open Systems Interconnection - Systems management: Alarm reporting function,” ITU-T X.733 (Normative Reference)
- [13] ”DOCSIS - Operations Support System Interface Specifications,” SP-OSSIV1.1-I01-000407, April 07, 2000, Cable Television Laboratories, Inc., <http://www.CableLabs.com/> (Informative Reference)

### 3 TERMS AND DEFINITIONS

This document uses the following terms and definitions.

<b>Network Layer</b>	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
<b>Network Management</b>	The functions related to the management of data across the network.
<b>Network Management OSS</b>	The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.

## 4 ABBREVIATIONS AND ACRONYMS

The PacketCable project uses the following abbreviations and acronyms.

<b>AAA</b>	Authentication, Authorization and Accounting
<b>AF</b>	Assured Forwarding. A Diffserv Per Hop Behavior.
<b>AH</b>	Authentication header is an IPSec security protocol that provides message integrity for complete IP packets, including the IP header.
<b>A-link</b>	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access".
<b>AMA</b>	Automated Message Accounting., a standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies)
<b>AT</b>	Access Tandem
<b>ATM</b>	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
<b>BAF</b>	Bellcore AMA Format, another way of saying AMA
<b>BPI+</b>	Baseline Privacy Interface Plus is the security portion of the DOCSIS 1.1 standard which runs on the MAC layer.
<b>CBC</b>	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.
<b>CBR</b>	Constant Bit Rate.
<b>CA</b>	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.
<b>CDR</b>	Call Detail Record. A single CDR is generated at the end of each billable activity. A single billable activity may also generate multiple CDRs
<b>CIC</b>	Circuit Identification Code. In ANSI SS7, a two octet number that uniquely identifies a DSO circuit within the scope of a single SS7 Point Code.
<b>CID</b>	Circuit ID (Pronounced "Kid"). This uniquely identifies an ISUP DSO circuit on a Media Gateway. It is a combination of the circuit's SS7 gateway point code and Circuit Identification Code (CIC). The SS7 DPC is associated with the Signaling Gateway that has domain over the circuit in question.
<b>CIF</b>	Common Intermediate Format
<b>CIR</b>	Committed Information Rate.
<b>CM</b>	DOCSIS Cable Modem.
<b>CMS</b>	Call Management Server. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology.
<b>CMTS</b>	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.
<b>Codec</b>	COder-DECoder
<b>COPS</b>	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.
<b>CoS</b>	Class of Service. The type 4 tuple of a DOCSIS 1.0 configuration file.

<b>CSR</b>	Customer Service Representative
<b>DA</b>	Directory Assistance
<b>DE</b>	Default. A Diffserv Per Hop Behavior.
<b>DHCP</b>	Dynamic Host Configuration Protocol.
<b>DHCP-D</b>	DHCP Default - Network Provider DHCP Server
<b>DNS</b>	Domain Name Server
<b>DSCP</b>	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.
<b>DOCSIS</b>	Data Over Cable System Interface Specification.
<b>DPC</b>	Destination Point Code. In ANSI SS7, a 3 octet number which uniquely identifies an SS7 Signaling Point, either an SSP, STP, or SCP.
<b>DQoS</b>	Dynamic Quality of Service, i.e. assigned on the fly for each communication depending on the QoS requested
<b>DTMF</b>	Dual-tone Multi Frequency (tones)
<b>EF</b>	Expedited Forwarding. A Diffserv Per Hop Behavior.
<b>E-MTA</b>	Embedded MTA – a single node which contains both an MTA and a cable modem.
<b>EO</b>	End Office
<b>ESP</b>	IPSec Encapsulation Security Payload protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
<b>ETSI</b>	European Telecommunications Standards Institute
<b>FGD</b>	Feature Group D signaling
<b>F-link</b>	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. ‘F’ stands for “Fully Associated”
<b>FQDN</b>	Fully Qualified Domain Name. Refer to IETF RFC 821 for details.
<b>H.323</b>	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.
<b>HFC</b>	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.
<b>H.GCP</b>	A protocol for media gateway control being developed by ITU.
<b>HMAC</b>	Hashed Message Authentication Code – a message authentication algorithm, based on either SHA-1 or MD5 hash and defined in RFC 2104.
<b>HTTP</b>	Hyper Text Transfer Protocol. Refer to IETF RFC 1945 and RFC 2068.
<b>IANA</b>	Internet Assigned Numbered Authority. See <a href="http://www.ietf.org">www.ietf.org</a> for details.
<b>IC</b>	Inter-exchange Carrier
<b>IETF</b>	Internet Engineering Task Force. A body responsible, among other things, for developing standards used in the Internet.
<b>IKE</b>	Internet Key Exchange is a key management mechanism used to negotiate and derive keys for SAs in IPSec.

<b>IKE-</b>	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
<b>IKE+</b>	A notation defined to refer to the use of IKE, which requires digital certificates for authentication.
<b>IP</b>	Internet Protocol. An Internet network-layer protocol.
<b>IPSec</b>	Internet Protocol Security, a collection of Internet standards for protecting IP packets with encryption and authentication.
<b>ISDN</b>	Integrated Services Digital Network
<b>ISUP</b>	ISDN User Part is a protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
<b>ISTP</b>	Internet Signaling Transport Protocol
<b>ISTP – User</b>	Any element, node, or software process that uses the ISTP stack for signaling communications.
<b>ITU</b>	International Telecommunication Union
<b>IVR</b>	Interactive Voice Response System
<b>LATA</b>	Local Access and Transport Area
<b>LD</b>	Long Distance
<b>LIDB</b>	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
<b>LLC</b>	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.
<b>LNP</b>	Local Number Portability. Allows a customer to retain the same number when switching from one local service provider to another.
<b>LSSGR</b>	LATA Switching Systems Generic Requirements
<b>MAC</b>	Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
<b>MC</b>	Multipoint Controller
<b>MD5</b>	Message Digest 5 - a one-way hash algorithm which maps variable length plaintext into fixed length (16 byte) ciphertext.
<b>MDCP</b>	A media gateway control specification submitted to IETF by Lucent. Now called SCTP.
<b>MDU</b>	Multi-Dwelling Unit. Multiple units within the same physical building. The term is usually associated with high rise buildings
<b>MEGACO</b>	Media Gateway Control IETF working group. See <a href="http://www.ietf.org">www.ietf.org</a> for details.
<b>MG</b>	The media gateway provides the bearer circuit interfaces to the PSTN and transcodes the media stream.
<b>MGC</b>	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.
<b>MGCP</b>	Media Gateway Control Protocol. Protocol follow on to SGCP.
<b>MIB</b>	Management Information Base
<b>MIC</b>	Message integrity code, a fixed length data item that is sent together with a message to ensure integrity, also known as a MAC.

<b>MMC</b>	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
<b>MSO</b>	Multi-System Operator, a cable company that operates many head-end locations in several cities.
<b>MSU</b>	Message Signal Unit
<b>MTA</b>	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.
<b>MTP</b>	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.
<b>MWD</b>	Maximum Waiting Delay
<b>NANP</b>	North American Numbering Plan
<b>NANPNAT</b>	North American Numbering Plan Network Address Translation
<b>NAT Network Layer</b>	Network Address Translation Layer 3 in the Open System Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.
<b>NCS</b>	Network Call Signaling
<b>NPA-NXX</b>	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP)
<b>NTP</b>	Network Time Protocol, an internet standard used for synchronizing clocks of elements distributed on an IP network
<b>NTSC</b>	National Television Standards Committee which defines the analog color television, broadcast standard used today in North America.
<b>OSP</b>	Operator Service Provider
<b>OSS-D</b>	OSS Default – Network Provider Provisioning Server
<b>OSS</b>	Operations Systems Support. The back office software used for configuration, performance, fault, accounting and security management.
<b>PAL</b>	Phase Alternate Line – the European color television format which evolved from the American NTSC standard.
<b>PDU</b>	Protocol Data Unit
<b>PKCS</b>	Public Key Cryptography Standards, published by RSA Data Security Inc. Describes how to use public key cryptography in a reliable, secure and interoperable way.
<b>PKI</b>	Public Key Infrastructure - a process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
<b>PKINIT</b>	The extension to the Kerberos protocol that provides a method for using public key cryptography during initial authentication.
<b>PHS</b>	Payload Header Suppression, a DOCSIS technique for compressing the Ethernet, IP and UDP headers of RTP packets.
<b>PSC</b>	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.

<b>PSFR</b>	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
<b>PSTN</b>	Public Switched Telephone Network.
<b>PCM</b>	Pulse Code Modulation – A commonly employed algorithm to digitize an analog signal (such as a human voice) into a digital bit stream using simple analog to digital conversion techniques.
<b>QCIF</b>	Quarter Common Intermediate Format
<b>QoS</b>	Quality of Service, guarantees network bandwidth and availability for applications.
<b>RADIUS</b>	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
<b>RAS</b>	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
<b>RC4</b>	A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in PacketCable.
<b>RFC</b>	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at <a href="http://www.ietf.cnri.reston.va.us/rfc.html">http://www.ietf.cnri.reston.va.us/rfc.html</a>
<b>RFI</b>	The DOCSIS Radio Frequency Interface specification.
<b>RJ-11</b>	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
<b>RKS</b>	Record Keeping Server, the device which collects and correlates the various Event Messages
<b>RSVP</b>	Resource reSerVation Protocol
<b>RTCP</b>	Real Time Control Protocol
<b>RTO</b>	Retransmission Timeout
<b>RTP</b>	Real Time Protocol, a protocol defined in RFC 1889 for encapsulating encoded voice and video streams.
<b>S-MTA</b>	Standalone MTA – a single node which contains an MTA and a non DOCSIS MAC (e.g. ethernet).
<b>SA</b>	Security Association - a one-way relationship between sender and receiver offering security services on the communication flow .
<b>SAID</b>	Security Association Identifier - uniquely identifies SAs in the BPI+ security protocol, part of the DOCSIS 1.1 specification.
<b>SCCP</b>	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.
<b>SCP</b>	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.
<b>SCTP</b>	Simple Control Transmission Protocol.
<b>SDP</b>	Session Description Protocol.

<b>SDU</b>	Service Data Unit. Information that is delivered as a unit between peer service access points.
<b>SF</b>	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
<b>SFID</b>	Service Flow ID, a 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. 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.
<b>SFR</b>	Service Flow Reference, a 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
<b>SG</b>	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
<b>SGCP</b>	Simple Gateway Control Protocol. Earlier draft of MGCP.
<b>SHA – 1</b>	Secure Hash Algorithm 1 - a one-way hash algorithm.
<b>SID</b>	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
<b>SIP</b>	Session Initiation Protocol is an application layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants.
<b>SIP+</b>	Session Initiation Protocol Plus is an extension to SIP.
<b>SNMP</b>	Simple Network Management Protocol
<b>SOHO</b>	Small Office/Home Office
<b>SPI</b>	Security Parameters Index - a field in the IPSEC header that along with the destination IP address provides a unique number for each SA.
<b>SS7</b>	Signaling System Number 7. SS7 is an architecture and set of protocols for performing out-of-band call signaling with a telephone network.
<b>SSP</b>	Signal Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
<b>STP</b>	Signal Transfer Point. 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.
<b>TCAP</b>	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling Control Point.
<b>TCP</b>	Transmission Control Protocol
<b>TD</b>	Timeout for Disconnect
<b>TFTP</b>	Trivial File Transfer Protocol
<b>TFTP-D</b>	Default – Trivial File Transfer Protocol
<b>TGS</b>	Ticket Granting Server used to grant Kerberos tickets.
<b>TGW</b>	Telephony Gateway

<b>TIPHON</b>	Telecommunications & Internet Protocol Harmonization Over Network.
<b>TLV</b>	Type-Length-Value tuple within a DOCSIS configuration file.
<b>TN</b>	Telephone Number
<b>ToD</b>	Time of Day Server
<b>TOS</b>	Type of Service. An 8-bit field of every IP version 4 packet. In a Diffserv domain, the TOS byte is treated as the Diffserv Code Point, or DSCP.
<b>TSG</b>	Trunk Subgroup
<b>UDP</b>	User Datagram Protocol, a connectionless protocol built upon Internet Protocol (IP).
<b>VAD</b>	Voice Activity Detection
<b>VBR</b>	Variable bit-rate
<b>VoIP</b>	Voice over IP
<b>WBEM</b>	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 <a href="http://www.dmtf.org">www.dmtf.org</a>

## 5 BACKGROUND

The PacketCable architecture is an end-end broadband architecture that supports voice, video, and other multimedia services. The individual components that compose the PacketCable architecture are defined in [1].

The OSS back office contains business, service, and network management components supporting the core business processes. The PacketCable OSS Framework Technical Report [2] provides a comprehensive diagram and detailed description of the OSS back office components including descriptions of EMS, NMS, and others.

The PacketCable set of specifications defines a limited set of OSS functional components and interfaces to support MTA device provisioning [6], Event Messaging to carry billing information [5], and the Management Event Mechanism defined in this document to carry fault and other data.

In addition to the Management Event Mechanism, the PacketCable architecture supports the following additional reporting mechanism:

- *PacketCable Events Messages for billing information [5]*. This reporting mechanism uses the RADIUS transport protocol, a pre-defined set of Event Message attributes (e.g. BillingCorrelationID, CalledPartyNumber, TrunkGroupID, etc.), and the PacketCable Event Messages data format to carry per-call information between PacketCable network elements (CMS, CMTS, MGC) and a Record Keeping Server (RKS). For each call, the RKS combines all associated Event Messages into a single Call Detail Record (CDR) which may be sent to a back office billing, fraud detection or other system. Vendor-proprietary data attributes may be included along with the PacketCable-defined set of attributes in a PacketCable Event Message.
- *Other Reporting Methods*. It is possible that PacketCable elements implement reporting methods specified in DOCSIS MIBs, PacketCable MIBs or other standard MIBs. It is possible that PacketCable elements implement methods such as SNMPv3, CMIP, TL1. These event-reporting mechanisms are not defined in this document.

## 6 PACKETCABLE 1.1 MANAGEMENT EVENT MECHANISM FUNCTIONAL REQUIREMENTS

The functional requirements addressed by the Message Event Mechanism specification are as follows:

1. An event report **MUST** provide the MAC address.
2. The event report **MUST** provide either the FQDN or IP address of the reporting device.
3. The PacketCable management event reporting mechanism **MUST** support 2 types of events: pre-defined and programmable. Examples of programmable events are the Primary Line telemetry events. Both PacketCable-specific and vendor-specific pre-defined events **MUST** be supported.
4. The management event reporting mechanism **MUST** support the provisioning and viewing of the programmable events.
5. The PacketCable management event reporting mechanism **MUST** support SYSLOG.
6. The management event reporting mechanism **MUST** support SNMPv3 Traps, SNMPv3 Informs.
7. The management event reporting mechanism **MUST** be able to integrate with the notification MIBs in RFC 2573 since these MIBs provide the mechanism for distributing SNMPv3 traps and informs. The elements **MUST** support a mechanism to allow the element management system to map each event to a reported notification mechanism(s). For example: none, local, SYSLOG, SNMPv3 Trap, SNMPv3 INFORM.
8. Each event **MUST** be uniquely identifiable to the point of origin such as a specific endpoint on an MTA.
9. The capability **SHOULD** exist to map event IDs to priorities in the back office.
10. PacketCable elements **MUST** send a timestamp with each management event.
11. PacketCable elements **MUST** send a Severity level with each management event. Elements **MAY** use the Severity level within the network element to determine the order in which events are sent in compliance with Bellcore GR474 section 2.2.3 and section 7.9.
12. The severity level of management events generated by the network element **MUST** be modifiable on the PacketCable element by the management system.

13. The display string of programmable management events generated by the PacketCable element MUST be modifiable on the network element by the management system.
14. A default notification mechanism MUST be associated with each event.
15. PacketCable-specific event definitions SHOULD contain a NULL display string in order to reduce memory requirements on the PacketCable element.
16. Programmable event definitions MUST contain a display string.
17. Vendor-specific event definitions MAY contain a NULL display string in order to reduce memory requirements on the PacketCable element.
18. Event throttling mechanism MUST be configurable by the management system.
19. All events are uniquely identified by vendor through the IANA assigned enterprise number. PacketCable events use the PacketCable IANA assigned enterprise number
20. An event MUST provide the Event ID of the event.

## 7 MANAGEMENT EVENT REPORTING MECHANISM

The Management Event Mechanism and the associated Management Event Mechanism MIB **MUST** be implemented on the MTA.

The Management Event Mechanism and the associated Management Event Mechanism MIB **MAY** be implemented on any PacketCable element such as the CMS, MGC, and others.

### 7.1 PacketCable Management Event Format

The format of a PacketCable Management Event is made up of the following information:

- Event Counter - indicator of event sequence
- Event Time - time of occurrence
- Event severity - severity of condition as defined in section 7.4
- Event Enterprise number – Vendor specific enterprise number
- Event ID - determines event function
- Event Text - describes the event in human readable form
- Mac Address – describes the MAC address of the device
- FQDN/Endpoint ID – describes the device FQDN and the specific endpoint associated with the event

### 7.2 PacketCable Management Event Access Method

The PacketCable event access methods is defined through the use of SNMPv3 in the case of local log access and trap or inform access. The SYSLOG uses UDP packets to convey the event data.

For local event log access, an EMS **MAY** send SNMP GET, GET-NEXT or GET-BULK requests to the PacketCable element, accessing rows of the local event table. Each row **MUST** contain the event data in the format as defined in section 7.1.

The SYSLOG method of accessing events involves sending the events to a SYSLOG server via the UDP protocol to the UDP SYSLOG port as defined in DOCSIS specification ‘SP-OSSIV1.1-I01-000407’. This event data **MUST** follow the event data format as defined in section 7.1.

The SNMPv3 Trap and Inform access methods involve defining a notification within the PacketCable MGMTEVENT MIB. The notification **MUST** contain the event data in the format as defined in section 7.1.

Any notification **MUST** be generated according to the entries in the associated SNMPv3 tables described in RFC 2573 in a vendor dependent manner. These provide the ability to address one or more management systems, the option to send traps or informs, and specify the security requirements for each management system.

## 7.3 Management Event ID

PacketCable management events are defined in an appendix of PacketCable specifications. Not all PacketCable specifications define management events. Each management event described in the appendix of a PacketCable specification is assigned a PacketCable Event ID. For a complete list of PacketCable Event IDs, refer to PKT-TR-MEMEVENT-ID-V01-0000929 [7].

## 7.4 Management Event Severities

Each event is assigned an initial (default) PacketCable MultiMedia-centric Severity. The definitions for the PacketCable MultiMedia-centric severities are loosely based on ITU-T M.3100 [11] and OSI System Management Alarm Reporting Function X.733 [12]. PacketCable expands on the definition provided in Bellcore's GR-474 (see section 7.9) to include the following list:

**critical(1)** – A service-affecting condition that requires immediate corrective action.

**major(2)** – A service-affecting condition that requires urgent corrective action.

**minor(3)** – A non-service-affecting fault condition which warrants corrective action in order to avoid a more serious fault.

**warning(4)** – A potential or impending condition which can lead to a fault; diagnostic action is suggested.

**information(5)** – Normal event meant to convey information.

Events, if they need to be cleared, **MUST** be cleared by other events.

Each application (e.g., DOCSIS, PacketCable) has its own event space. There is no predetermined relationship of event severity defined or enforced between application.

When managing events that affect multiple applications two scenarios are possible. They are as follows:

1. A particular application is considered the master. The master application sends the multiple destination events to its element manager. The application's element manages then broadcasts that event to all other element managers that are interested in that event. Severity translation is vendor dependent.
2. When an event occurs, every application interested in that event has its own event notification data template defined. An event is then sent out by each interested application according to its event notification data template.

Event vendor in conjunction with the MSOs will implement its mechanism based on one of the scenarios described above.

### 7.4.1 Changing Default Event Severities

The default event severity **MUST** be changeable to a different value for each given event via the SNMP interface.

## 7.5 Programmable Events

### 7.5.1 Description

A programmable event is an event that looks at stimulus within or external to an element. The stimulus does not necessarily have a predefined definition among all MSOs or sites. The programming of these events is MSO dependent and **MUST** have a display string that defines what occurs, such as “power fail”. For example, the MTA **MAY** support a programmable event with event ID of SNMP TELEMETRY\_EV1, default display string of “AC Power Fail” and a default Severity of Critical.

### 7.5.2 Default Display String Change Mechanism

The default display string text **MUST** be changeable via the SNMP interface.

## 7.6 Notification Mechanism

The notification mechanism for each event **MUST** be programmable via the SNMP interface.

Each event **MUST** be able to be sent to one or more notification mechanisms.

The notification mechanism definitions are as follows:

- local: The event is stored locally on the device in which it is generated. The event can be retrieved via polling from the SNMP agent interface.
- trap: The event is sent via the SNMPv3 TRAP mechanism to the targeted management systems. Due to the unacknowledged nature of the SNMPv3 TRAP mechanism, these event notifications are not guaranteed to be delivered to the targeted management systems.
- inform: The event is sent via the SNMPv3 INFORM mechanism to the targeted management systems. Since the SNMPv3 INFORM mechanism is acknowledged, these events will be reliably transmitted to the targeted management systems.
- syslog: The event is sent to the SYSLOG server.
- none: No reporting action is taken, this is the equivalent of disabling the event. If “none” is specified, the other notification mechanism choices **MUST** be ignored.

## 7.7 Local Log of Events

The local log **MUST** be accessed via SNMP using the objects defined in the MGMTEVENT MIB. A vendor may provide alternative access procedures.

## 7.8 Event Throttling

Throttling is implemented globally through a rate based threshold mechanism, as defined in the PacketCable MGMTEVENT MIB.

Control of the throttling mechanism is through a MIB object that specifies one of four states.

- Event generation inhibited – events defined through the event mechanism are no longer sent via syslog, traps, or informs.
- Throttling inhibited – events are sent without any throttling.
- Dynamic thresholding enabled – threshold based throttling is enabled
- Manual thresholding enabled – manual intervention is required to resume event generation after crossing the initial threshold halts event generation.

Manual intervention through setting a MIB object is used to resume event generation when manual thresholding is enabled.

Inhibiting the generation of events **MUST** be handled through the use of the MIB objects, one to specify a number of events, and one to specify a time period over which those events are generated. The default frequency is defined as 2 events per second in the MGMTEVENT MIB. When event generation exceeds this rate, no more events are sent via SYSLOG, traps, or informs. The throttling of Local logging of events is vendor specific.

Dynamic thresholding requires setting MIB objects to resume events. One object specifies the number of events, and the other is the time period object specified above. The default frequency is defined as 1 event per second. This defines the rate at which event generation is resumed.

Threshold settings are not persistent, and **MUST** be reinitialized when the PacketCable element reboots.

In addition to this mechanism, vendors may support other throttling mechanisms.

## 7.9 Severity and Priority Definition

**Severity** is the degree of failure related to a specific event by a reporting device. Bellcore document GR-474-CORE [10], Network Maintenance: Alarm and Control for Network Elements defines three degrees of severity:

- Critical – Used to indicate a severe, service-affecting condition has occurred and that immediate corrective action is imperative, regardless of the time of day or day of the week.
- Major – Used for hardware and software conditions that indicate a serious disruption of service or the malfunctioning or failure of important circuits. These troubles require the immediate attention and response of a craftsperson to restore or maintain system capability. The urgency is less than in critical situations because of a lesser immediate or impending effect on service or system performance.
- Minor – Used for troubles that do not have a serious effect on service to customers or for troubles in circuits that are not essential to Network Element operation.

**Priority** is the precedence established by order of importance or urgency. The back office manages the priority of how and when a particular event is serviced based on

the severity of the reported event. According to Bellcore GR-474-CORE [10], Network Maintenance: Alarm and Control for Network Elements, the following priority sequences for trouble notifications shall prevail:

- Critical alarms have the highest priority and shall be serviced before any major or minor alarms.
- Major alarms have higher priority than minor alarms and shall be serviced before any minor alarms.
- Minor alarms shall be serviced before non-alarmed trouble notifications.

## 8 PACKETCABLE MANAGEMENT EVENT DATA TEMPLATE

In order to ensure multi-vendor interoperability of network management functionality, the specific meaning of PacketCable management events are defined. Because the PacketCable management events are based on conditions identified in PacketCable specifications, management events are defined in the appendix of the appropriate PacketCable specifications.

The following table shows the data required to describe the meaning of PacketCable management events. The data contained in this table is for informational purposes only, this table will contain specific data when added to the appendix of a PacketCable specification.

Example management Event Data						
Enterprise Number	Event Name	Default Severity for event raises	Default Display String	Comments	Programmable / Pre-Defined	Associated Events
4491	PL-EV-1	minor	“AC Power Fail”	Telemetry pin 1 has been asserted.	Programmable	PL-EV-2
4491	PL-EV-2	minor	“AC Power Restore”	Telemetry pin 1 has been de-asserted.	Programmable	PL-EV-1
4491	PROV-EV-1	major	“MTA Missing Name”	The MTA was not provisioned with an FQDN.	Pre-defined	none

## Appendix A. Acknowledgements

The PacketCable project would like to thank and formally acknowledge the significant contributions of the Provisioning Team group who helped formulate the initial draft of this document. Those contributors include the following individuals and companies:

Angela Lyda and Rick Morris (Arris), Maria Stachelek (CableLabs), Mike Fenlon and Klaus Hermanns (Cisco), Rick Vetter (Motorola), Brenda Conner and Kevin Ball (Ericsson), Ghislaine Griswold, David Walters and Roger Loots (Lucent), and Roy Spitzer (Telogy).

*Matthew A. Osman, CableLabs*

## Appendix B. Revisions

### Engineering Change Numbers

ECN	Date Ratified	Summary