Society of Cable Telecommunications Engineers

ENGINEERING COMMITTEE
Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 165-16 2016

IPCablecom 1.5 Part 16: Management Event Mechanism

NOTICE

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

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

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

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

140 Philips Road
Exton, PA 19341

Note: DOCSIS® and PacketCable™ are registered trademarks of Cable Television Laboratories, Inc., and are used in this document with permission.

Contents

Tables

This page intentionally left blank.

1 INTRODUCTION

1.1 Purpose

This standard defines the Management Event Mechanism that IPCablecom elements can use to report asynchronous events that indicate malfunction situations and notification about important non-fault situation.

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

A goal of IPCablecom is to maintain consistency with the DOCSIS® event reporting mechanism [6].

1.2 Scope

This standard is one of two documents that together define a framework for reporting Management Events in the IPCablecom architecture.

This document 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 IPCablecom architecture. This document defines how the SNMPv3 transport protocol, SYSLOG, local log, and the IPCablecom Management Event MIB are used to carry management event information to an event management system.

This management event mechanism is further defined and supported by the Management Event Mechanism MIB as specified in [1], and [13] if the latter is implemented by the MTA. Consequently, each reference to the Management Event MIB in this document will correspond to the MIB as defined either in [1], or alternatively, in [1] and [13].

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 IPCablecom 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, event descriptions, notification mechanism, local log of events, event throttling, and definition of severities and priorities.
- Section 8 – Example template for the management data.
- Appendix A – IPCablecom-defined provisioning events.
- Appendix B – IPCablecom-defined powering events.
- Appendix C – PacketCable-defined Diagnostic Events

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 an IPCablecom 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

The following documents contain provisions which, through reference in this text, constitute provisions of this standard. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision, and while parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1 Normative References

In order to claim compliance with this standard, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this standard. Intellectual property rights may be required to implement these references.

[1] SCTE 165-15 2016, IPCablecom 1.5 Part 15: Management Event MIB Specification.

[2] SCTE 165-09 2016, IPCablecom 1.5 Part 9: Event Messages.

[3] SCTE 165-19 2016, IPCablecom 1.5 Part 19: CMS Subscriber Provisioning Specification.

[4] SCTE 165-07 2016, IPCablecom 1.5 Part 7: MTA MIB.

[5] SCTE 165-14 2016, IPCablecom 1.5 Part 14: Embedded MTA Analog Interface and Powering.

[6] ANSI/SCTE 23-03 2012, DOCSIS 1.1 Part 3: Operations Support System Interface

[7] IETF RFC 3413/STD0062, Simple Network Management Protocol (SNMP) Applications, December 2002.

[8] IETF RFC 3164, The BSD Syslog Protocol, August 2001.

2.2 Informative References

The following documents may provide valuable information to the reader but are not required when complying with this standard.

[9] ANSI/SCTE 165-1 2016, IPCablecom 1.5 Part 1: Architecture Framework Technical Report.

[10] Network Maintenance: Alarm and Control for Network Elements, Bellcore GR-474.

[11] ITU-T Recommendation M.3100, Generic Network Information Model, 1995.

[12] ITU-T Recommendation X.733, Open Systems Interconnection - Systems management: Alarm reporting function, 1992.

[13] IETF RFC5428, Management Event Management Information Base (MIB) for PacketCable- and IPCablecom-Compliant Devices, April 2009.

[14] IETF RFC5234, Augmented BNF for Syntax Specifications: ABNF, January 2008.

[15] IETF RFC2131, Dynamic Host Configuration Protocol, March 1997.

2.3 Reference Acquisition

- Internet Engineering Task Force (IETF) Secretariat c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA 20191-5434, Phone +1-703-620-8990, Fax +1-703-620-9071, Internet: www.ietf.org/
- ITU available at http://www.itu.int/ITU-T/publications/index.html

3 TERMS AND DEFINITIONS

This document uses the following terms and definitions.

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.

4 ABBREVIATIONS AND ACRONYMS

This IPCablecom document uses the following abbreviations and acronyms.

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.

FQDN Fully Qualified Domain Name. Refer to IETF RFC 821 for details.

IANA Internet Assigned Numbered Authority. See www.ietf.org for details.

MAC Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.

MGC A Media Gateway Controller is the overall controller function of the PSTN gateway. It receives, controls and mediates call signaling information between the IPCablecom and PSTN.

MIB Management Information Base

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.

OSP Operator Service Provider

SNMP Simple Network Management Protocol

UDP User Datagram Protocol, a connectionless protocol built upon Internet Protocol (IP).

5 BACKGROUND

The IPCablecom architecture is an end-end broadband architecture that supports voice, video, and other multimedia services. The individual components that compose the IPCablecom architecture are defined in [9].

The OSS back office contains business, service, and network management components supporting the core business processes. The IPCablecom set of specifications defines a limited set of OSS functional components and interfaces to support MTA Device Provisioning [3], Event Messaging to carry billing information [2], and the Management Event Mechanism defined in this document to carry fault and other data.

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

- IPCablecom Events Messages for billing information [2]. This reporting mechanism uses the RADIUS transport protocol, a pre-defined set of Event Message attributes (e.g., BillingCorrelationID, CalledPartyNumber, TrunkGroupID, etc.), and the IPCablecom Event Messages data format to carry per-call information between IPCablecom 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 IPCablecom-defined set of attributes in an IPCablecom Event Message.
- *Other Reporting Methods*. It is possible that IPCablecom elements implement reporting methods specified in DOCSIS MIBs, IPCablecom MIBs or other standard MIBs. It is possible that IPCablecom elements implement methods such as SNMPv3, CMIP, TL1. These event-reporting mechanisms are not defined in this document.

6 IPCABLECOM MANAGEMENT EVENT MECHANISM FUNCTIONAL REQUIREMENTS

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

1. The event report MUST provide either the FQDN or IP address of the reporting device.
   (Note: It is highly recommended that the device provide the FQDN.)
2. The IPCablecom management event reporting mechanism MUST support 2 types of events: IPCablecom-specific and Vendor-specific.
3. The management event reporting mechanism MUST support the IPCablecom 1.5 Management Event MIB [1]. All the events that can be generated by the IPCablecom device MUST be included in the MIB table 'pktcDevEventDescrTable'.
4. The IPCablecom management event reporting mechanism MUST support the BSD syslog protocol [8].
5. The management event reporting mechanism MUST support SNMPv3/v2c Traps and SNMPv3/v2c Informs.
6. The management event reporting mechanism MUST comply with SNMP Applications [7] 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/v2c Trap, SNMPv3/v2c INFORM.

   Note: Refer to the IPCablecom 1.5 MTA Device Provisioning Specification [3] for more information about SNMP configuration.
7. Each event MUST be uniquely identifiable to the point of origin such as a specific endpoint on an MTA.
8. The capability SHOULD exist to map event IDs to priorities in the back office.
9. IPCablecom elements MUST send a timestamp with each management event.
10. IPCablecom 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's Section 2.2.3 and Section 7.10 of this document.
11. The severity level of management events generated by the network element MUST be modifiable on the IPCablecom element by the management system.
12. The display string of management events generated by the IPCablecom element MUST be modifiable on the network element by the management system.
13. A default notification mechanism MUST be associated with each event.
14. IPCablecom-specific event definitions SHOULD contain a NULL display string in order to reduce memory requirements on the IPCablecom element.
15. Event definitions MUST contain a display string.
16. Vendor-specific event definitions MAY contain a NULL display string in order to reduce memory requirements on the IPCablecom element.
17. Event throttling mechanism MUST be configurable by the management system.
18. All events are uniquely identified by vendor through the IANA assigned enterprise number. IPCablecom events use the CableLabs IANA assigned enterprise number.
19. An event MUST provide the Event ID of the event.

7 MANAGEMENT EVENT REPORTING MECHANISM

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

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

7.1 Event Notification Categories

All events delivered by (event mechanism document) fit into two main categories:

- IPCablecom-specific
- Vendor-specific

IPCablecom-specific events are defined in this document and referenced by concerned specifications whereas vendor-specific events are left to vendor implementation and are out of scope of this specification.

Each Event has an associated Event ID as described in the next sub-section. IPCablecom-Specific events are identical if their EventIDs are identical. The IPCablecom-Specific EventIDs are specified by the IPCablecom Specifications, including this specification. For each particular vendor, Vendor-specific events are identical if the corresponding Event IDs are identical. The Vendor-specific EventIDs are defined by particular vendors and is out of scope for this specification.

Example:

> Two or more IPCablecom Events with the same Event ID (Say 4000950100) are considered to be identical irrespective of the description or other parameters.
>
> Two or more Vendor-Specific Events, from the same vendor (Say XYZ) with the same Event ID (Say 10) are considered to be identical irrespective of the description or other parameters.

For identical events occurring consecutively, the MTA MAY choose to store only a single event. In such a case, the event description recorded MUST reflect the most recent event.

Aside from the procedures defined in this document, event recording MUST conform to the requirements of [1] and Event Descriptions MUST not be longer than 127 characters.

7.1.1 Event ID Assignments

- The EventID is a 32-bit unsigned integer.
- IPCablecom-specific EventIDs MUST be defined in the range of 0x80000000 (decimal 2,147,483,648) to 0xFFFFFFFF (decimal 4,294,967,295).
- Vendor-specific EventIDs MUST be defined in the range of 0x00000000 (decimal 0) to 0x7FFFFFFF (decimal 2,147,483,647).
- Vendor-specific EventIDs MUST be unique for a particular vendor's enterprise number in sysObjectID.

7.2 IPCablecom Management Event Format

The format of an IPCablecom 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 7.5
- Event Enterprise number – Vendor specific enterprise number
- Event ID - determines event function

- Event Text - describes the event in human readable form
- FQDN/Endpoint ID – describes the device FQDN and the specific endpoint associated with the event

Appendix A and Appendix C specify a number of events that are dependent on the conditions leading to the event. For such events the eMTA MUST format the "Event Text" field in compliance with the following definitions in ABNF (Augmented Backus-Naur Form (see [14]) and the associated requirements and comments:

PROV-EV-16

```
<PROV-EV-16> = "DHCP ERROR:" dhcp-message ";" dhcp-state [";"error-info] [";" ip-address-list]
dhcp-message = "DISCOVER" / "OFFER" / "REQUEST"/ "ACK" / "NAK"
dhcp-state = "INIT-REBOOT" / "REBOOTING" / "INIT" / "SELECTING" / "REQUESTING" /  "REBINDING" /
"BOUND" / "RENEWING"
error-info = 1*(VCHAR)
ip-address-list = ip-address ["," (ip-address)]
ip-address = 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT
```

Notes:
For the outbound DHCP messages, the eMTA MUST create the PROV-EV-16 events when the DHCP message cannot be generated or sent by the eMTA for any reason. For the inbound DHCP messages, the eMTA MUST create the PROV-EV-16 events when either the corresponding DHCP message is expected but has not been received (e.g., no DHCP OFFER messages were received within the expected timeout) or when it has been received but contains any errors in its contents or semantics (e.g., the DHCP ACK message contains an ill-formed option 122).

The <dhcp-state> field indicates the state of the eMTA’s DHCP state machine, the eMTA was in when the error occurred. The meaning and designation of the states are according to [15].

The optional <error-info> field represents the ASCII string containing the human readable information on the details of the error. For example:

The optional <ip-address-list> contains the list of the IPv4 addresses of the DHCP Servers, which are related to the error.

The following are examples of the PROV-EV-16 events:

- “DHCP ERROR: ACK;REQUESTING;Option 122 from DHCP Server is not correctly formatted; 1.2.3.4”.
- “DHCP ERROR: ACK; REBINDING; NAK received when ACK expected; 1.2.3.4”

DIAG-EV-1

```
<DIAG-EV-1> = "MEM-CONN-ERROR" [";"error-info]
error-info = 1*(VCHAR)
; <error-info> contains information identifying the particular reason for the loss of
connectivity (e.g., no IP address)
```

DIAG-EV-2

```
<DIAG-EV-2> = "MTA RESET:" reset-reason ":" max-number-of-events-stored [";"error-info]
reset-reason = "CLI" / "CM" / "SNMP"/ "PROACTIVE" / "UNKNOWN"
max-number-of-events-stored = *(DIGIT)
;this is the maximum number of events (irrespective of the severity) that the MTA is capable of
recording in non-volatile storage. For MTAs that support non-volatile event storage, this number
needs to be equal to, or greater than 32 (per Section Error! Reference source not found.)
error-info = 1*(VCHAR)
;The <reset-reason> field can have the following values:
; CLI – reset due to the user instruction via a command-line -interface;
; CM – reset due to the eCM reset.
; SNMP – eMTA reset due to the PacketCable SNMP management request.
; PROACTIVE – eMTA reset due to the any known reasons, which can be identified
; by the eMTA (e.g. "watch-dog" timer expiration).
; UNKNOWN –  eMTA reset reason is unknown. For example, resets due to internal reasons related
; to the software or hardware malfunction, etc.
; optional <error-info> field can contain any additional debug information that the MTA can
provide.
; The eMTA MUST fill <error-info> field when the <reset-reason> is set to a value of PROACTIVE.
```

DIAG-EV-3

```
<DIAG-EV-3> = "ENDPT-HW-ERROR" [";"error-info]
error-info = 1*(VCHAR)
; <error-info> field contains the additional information identifying the particular reason of the
error to appear.
```

DIAG-EV-4

```
<DIAG-EV-4> = "DOCSIS-CONN-ERROR" [";"error-info]
error-info = 1*(VCHAR)
; <error-info> contains information identifying the particular reason for the loss of
connectivity
; (e.g. T3 or T4 timeouts, SF deleted) along with any additional details of the error cause.
```

7.3 IPCablecom Management Event Access Method

The IPCablecom event access method 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 IPCablecom 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 [6]. 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 IPCablecom Management Event 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.

7.4 Management Event ID

IPCablecom management events are defined in an appendix of IPCablecom specifications. Not all IPCablecom specifications define management events. Each management event described in the appendix of an IPCablecom specification is assigned an IPCablecom Event ID. For a complete list of IPCablecom Event IDs, refer to Appendix A and Appendix B in this document.

7.5 Management Event Severities

Each event is assigned an initial (default) IPCablecom MultiMedia-centric Severity. The definitions for the IPCablecom MultiMedia-centric severities are loosely based on ITU-T M.3100 [11] and OSI System Management Alarm Reporting Function X.733 [12]. IPCablecom expands on the definition provided in Bellcore's GR-474 (see Section 7.10) 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, IPCablecom) has its own event space. There is no predetermined relationship of event severity defined or enforced between applications.

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.

7.5.1 Changing Default Event Severities

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

7.6 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.

Whenever the specified condition in the MTA functionality occurs, the MTA MUST do the following: create and format the corresponding event (as per section 7.2), record the event in the local volatile or non-volatile storage (i.e., as specified in [1]), verify the transmission requirements (per [1]), and, if configured, send the event via syslog and/or SNMP immediately within the applicable threshold parameters (as specified in [1]).

There are times when the MTA may be unable to transmit an event (via syslog or SNMP) due to loss of connectivity, which is specified as one of the following conditions:

MTA has no IP address (e.g., events that occur during the DHCP process, or an MTA reset);

MTA cannot transmit IP packets for any reason (e.g., IP stack failures);

- MTA cannot successfully send an SNMP INFORM after retries (i.e., does not get an acknowledgement) and syslog is not configured.

In such cases (i.e., loss of connectivity, as specified above), if NV-Events (as specified in Section 7.7) did occur and were not transmitted, the MTA MUST create DIAG-EV-1 and send it immediately after connectivity is restored. Further, when the MTA transmits DIAG-EV-1, it MUST NOT send any of the events that occurred previously that were not transmitted. This does not preclude an MTA from sending any events that are created after connectivity was established. The MTA MUST NOT use DIAG-EV-1 for events other than NV-Events (as specified in Section 7.7).

7.7 Local Log of Events

The MTA MUST support local logging of events. The local log MUST be accessed via SNMP using the objects defined in the [1]. A vendor may provide alternative access procedures.

The MTA MAY implement local logging either in volatile memory, non-volatile memory or both. The index provided in [1] provides relative ordering of events in the log. The creation of local volatile and local-nonvolatile logs necessitates a method for synchronizing index values between the two local logs after reboot. If both volatile and non-volatile logs are maintained then the following procedure MUST be used after reboot:

- the values of the index maintained in the local non-volatile log MUST be renumbered beginning with one.
- the local volatile log MUST then be initialized with the contents of the local non volatile log.
- the first event recorded in the new active session's local-volatile log MUST use as its index, an increment by one of the last restored non-volatile index.

Also, a reset of the log initiated through an SNMP SET operation applied to the corresponding MIB objects of the Management Event MIB MUST clear both the local-volatile and local-nonvolatile logs.

An MTA MAY use the non-volatile event storage to implement the local logging of events. An MTA that supports non-volatile event storage MUST be able to persist at least 32 events across reboots or resets. The MTA MUST store events in reverse chronological order, i.e., the most recent events are always stored. Additionally, if an MTA supports recording of events in non-volatile memory then it MUST support storing of the following subset of the events in non-volatile storage (referred to as "NV-Events"):

- all MEM events with a severity of ‘emergency’, ‘alert’, ‘critical’ and ‘error’ (per [1])
- PL-EV-1
- PL-EV-2
- PROV-EV-15

All other events MAY be stored in non-volatile storage. An MTA MUST make sure that all the NV-Events are given priority over events of other severity (e.g., informational). For example, consider an MTA which supports storage of 32 events. The MTA reaches this limit at some point in time. When a new event of category "NV-Events" occurs, there are two possible scenarios:

- if the MTA has previously stored an event that is ‘informational’ then the new event is stored (in non-volatile storage) and the ‘informational’ event removed;
- if the MTA has only NV-Events then the new event replaces the oldest event (i.e., storage is in chronological order, and the most recent events are stored).

If the MTA has sufficient non-volatile storage space to store all events, then it MAY do so.

The Management Event Mechanism (MEM) MIB [1] also specifies the event transmission requirements (i.e., to transmit or not) and the mechanisms for transmission (i.e., local log, syslog, SNMP trap, SNMP inform). Thus, whenever a specified event occurs, the MTA MUST do the following: record the event in the log (i.e., within), verify the transmission requirements (within [1]) and if configured to transmit the event via syslog or SNMP, attempt to send it across immediately within the applicable threshold parameters (as specified in [1]).

7.8 Syslog

All Syslog messages sent by an IPCablecom eMTA MUST comply with the following requirements:

- It MUST use UDP as the transport mechanism with 514 as the destination port as defined in Section 2 of the BSD syslog protocol [8].

- It SHOULD use port 514 as the source port, as recommended in Section 2 of SNMP applications [8].
- It MUST comply with the Packet Format and Contents as defined in Section 4 of [8] as applicable to the origination of the message and use the format as described in the following sub-section.

7.8.1 Syslog Message Format

This sub-section defines the usage of the Syslog fields as defined in Section 4 of [8].

7.8.2 PRI Part of a Syslog Packet

For the PRI part defined in Section 4.1.1 the facility to use MUST be:

16 local use 0 (local0)

The severity is the severity as indicated in the definition of the Event message (0-7).

The 'Priority Code' is as defined in Section 4.1 and ranges between 128 and 135 for IPCablecom.

7.8.3 MSG Part of a Syslog Packet

The MTA MUST include the following components:

TIMESTAMP, HOSTNAME, TAG and the CONTEXT.

Where

- TIMESTAMP is the time recorded by the MTA. (This MUST reflect the time in UTC as obtained from the Cable Modem).
- HOSTNAME MUST be the hostname received by the MTA in Option 12 of the DHCP ACK. (Refer to [3] for more details).
- The TAG field MUST be set to the string 'MTA', without the quotes.
- The PID field MUST be implemented and used as an 'Event Type Identifier'. The value MUST be: PacketCable for all Packetcable defined Event Messages.
- A vendor-specific unique identifier for vendor-defined Event Messages. While the vendor-specific choices are out of scope of this specification, a vendor MUST use the same unique identifier for all messages originating from a device.
- The CONTEXT part of the message MUST be formatted as follows: <eventID><correlationID> Description. Where:
- eventID MUST be the Event ID defined for each Event Message enclosed within angular braces.
- correlationID MUST the correlation ID generated by the MTA as defined in Section 5.4.5 of the Device Provisioning specification [3].
- Description MUST be the description associated for the particular event as stored in the Management Event MIB [1].

Example 1:

PROV-EV-1 is a PacketCable defined 'Event', defined as follows:

Table 1 - Example IPCablecom defined Event

Event Name	Event Priority	Default Display String	IPCablecom EventID	Comments
PROV-EV-1	Critical	"Waiting for DNS Resolution of Provisioning Realm Name"	4000950100	A DNS SRV Request has been transmitted for requesting the Provisioning Realm Information, but no response has been received from the DNS server.

Assuming that the MTA has been requested to send SYSLOG messages (Refer to [3] and [1] for more information on turning on SYSLOG messages):

- The Event Priority for critical is 2 (Refer to [1] for more information) and hence the 'Priority Code' is 130.
- Since this is an PacketCable Defined event, the 'Event Type Identifier' is 'PACKETCABLE'.
- The defined Event ID is 4000967295 and the assuming the default string has not been changed, the associated text is 'Waiting for Provisioning Realm Name DNS Resolution'.
- Assume the hostname to be CL_mta_1 and a correlation ID of 100

Thus, the event, if triggered will be sent as the following SYSLOG message:

```
<130>Jan  1 09:00:00 CL_mta_1 MTA[PACKETCABLE]:<4000850100><100>
Waiting for DNS Resolution of Provisioning Realm Name.
```

Example 2:

Assume the following hypothetical vendor-specific event defined by vendor 'XYZ Inc', with vendor ID 'XYZ'.

Table 2 - Example Vendor-specific Event

Event Name	Event Priority	Display String	Vendor Specific EventID	Comments
XYZ-EV-1	Warning	"AC Power Failure; running on battery"	10	AC Power Failure occurred and the device is running on battery power.

Again, assuming that the MTA has been requested to send SYSLOG messages (Refer to [3] and [1] for more information on turning on SYSLOG messages):

- The Event Priority for warning is 4 (Refer to [1] for more information) and hence the 'Priority Code' is 132.
- Vendor ID is 'XYZ' as stated in the example.
- The defined Event ID is 10 and the display string as indicated is: 'AC Power Failure; running on battery'.
- Assume the hostname to be CL_mta_2 and a correlation ID of 150

Thus, the event, if triggered will be sent as the following SYSLOG message:

```
<132> Jan 11 21:04:03 CL_mta_2 MTA[XYZ]:<10><150>AC Power Failure; running on battery
```

7.9 Event Throttling

Throttling is implemented globally through a rate based threshold mechanism, as defined in the PacketCable Management Event 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 two events per second in the Management Event 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 one event per second. This defines the rate at which event generation is resumed.

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

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

7.10 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 IPCablecom specifications, management events are defined in the separate appendices of this document.

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

Table 3 - Example Management Event Data

Enterprise Number	Event Name	Default Severity for event raises	Default Display String	Comments	Associated Events
4491	PL-EV-1	informational	"AC Power Fail"	Telemetry pin 1 has been asserted.	PL-EV-2
4491	PL-EV-2	informational	"AC Power Restore"	Telemetry pin 1 has been de-asserted.	PL-EV-1
4491	PROV-EV-1	error	"MTA Missing Name"	The MTA was not provisioned with an FQDN.	none

Appendix A PacketCable-defined Provisioning Events

Note: For sake of simplicity and continuity Event IDs from 4000950100 upwards are reserved for Provisioning Events.

Table 4 - Provisioning Events

Event Name	Default Severity for Event	Default Display String	IPCablecom EventID	Comments
PROV-EV-1	Error	"Waiting for DNS Resolution of Provisioning Realm Name"	4000950100	A DNS SRV Request has been transmitted for requesting the Provisioning Realm Information, but no response has been received from the DNS server.
PROV-EV-1.1	Critical	"Provisioning Realm Name unknown to the DNS Server"	4000950101	The DNS SRV Response from the DNS server did not resolve the Provisioning Realm Name.
PROV-EV-2	Error	"Waiting for DNS resolution of MSO/Provisioning KDC FQDN"	4000950200	A DNS Request has been transmitted to request the MSO KDC (or Provisioning KDC) FQDN, but no response has been received.
PROV-EV-2.1	Critical	"MSO/Provisioning KDC FQDN unknown to the DNS Server"	4000950201	The DNS Response from the DNS server did not resolve the MSO/Provisioning KDC FQDN.
PROV-EV-3	Error	"Waiting For MSO/Provisioning KDC AS Reply"	4000950300	A Kerberos AS Request has been transmitted to the MSO KDC (or Provisioning KDC), but no AS Response has been received.
PROV-EV-2.2	Error	“Waiting for DNS resolution of Provisioning Server FQDN”	4000950202	A DNS Request has been transmitted to request the Provisioning Server FQDN, but no response has been received.
PROV-EV-2.3	Critical	“Provisioning Server FQDN unknown to the DNS Server”	4000950203	The DNS Response from the DNS server did not resolve the Provisioning Server FQDN.
PROV-EV-3.1	Warning	"MSO/Provisioning KDC did not accept the AS Request"	4000950301	The Kerberos MSO/Provisioning KDC rejected the AS-Request (KRB_ERROR)
PROV-EV-4	Error	"Waiting For MSO/Provisioning KDC TGS Reply"	4000950400	A Kerberos TGS Request has been transmitted to the MSO KDC (or Provisioning KDC), but no TGS Response has been received.
PROV-EV-4.1	Warning	"MSO/Provisioning KDC did not accept AS Request"	4000950401	The MSO/Provisioning KDC rejected the Kerberos AS Request. (KRB_ERROR)

Event Name	Default Severity for Event	Default Display String	IPCablecom EventID	Comments
PROV-EV-5	Critical	"Waiting for Provisioning Server AP Reply"	4000950500	A Kerberos AP Request has been transmitted to the MSO Provisioning Server (SNMP Entity), but no AP Response has been received.
PROV-EV-5.1	Warning	"Provisioning Server/SNMP Entity rejected the Provisioning AP Request"	4000950501	The Provisioning Server/SNMP Entity rejected the Kerberos AP Request. (KRB_ERROR)
PROV-EV-6	Critical	"SNMPv3 INFORM transmitted; Waiting for SNMPv3 GET and/or SNMPv3 SET messages"	4000950600	SNMPv3 INFORM message has been transmitted and the device is waiting on optional (iterative) SNMv3 GET requests or an SNMPv3 SET.
PROV-EV-6.1	Critical	"SNMPv2c INFORM transmitted; Waiting for SNMPv2c GET and/or SNMPv2c SET messages"	4000950601	SNMPv2c INFORM message has been transmitted and the device is waiting on optional (iterative) SNMv2c GET requests or an SNMPv2c SET.
PROV-EV-8	Error	"Waiting For DNS Resolution of TFTP FQDN"	4000950800	A DNS Request has been transmitted to request the TFTP FQDN, but no response has been received.
PROV-EV-8.1	Critical	"TFTP FQDN unknown to the DNS Server"	4000950801	The DNS Response from the DNS server did not resolve the TFTP FQDN.
PROV-EV-9	Critical	"Waiting for TFTP Response"	4000950900	A TFTP request has been transmitted and no response has been received. (This could be for any TFTP Request during the download process).
PROV-EV-9.1	Critical	"Configuration File Error – Bad Authentication"	4000950901	The config file authentication value did not agree with the value in pktcMtaDevProvConfigHash or the authentication parameters were invalid.
PROV-EV-9.2	Critical	"Configuration File Error – Bad Privacy"	4000950902	The privacy parameters were invalid.
PROV-EV-9.3	Critical	"Configuration File Error – Bad Format"	4000950903	The format of the configuration file was not as expected.
PROV-EV-9.4	Critical	"Configuration File Error – Missing Parameter"	4000950904	Mandatory parameter of the configuration file is missing.

Event Name	Default Severity for Event	Default Display String	IPCablecom EventID	Comments
PROV-EV-9.5	Error	"Configuration File Error– Bad Parameter"	4000950905	Parameter within the configuration file had a bad value.
PROV-EV-9.6	Error	"Configuration File Error– Bad Linkage"	4000950906	Table linkages in the configuration file could not be resolved.
PROV-EV-9.7	Error	“Configuration File Error– Misc.”	4000950907	Configuration File error - Miscellaneous.
PROV-EV-12	Warning	"Telephony KDC did not accept AS Request"	4000951200	The Telephony KDC rejected the AS-Request (KRB_ERROR)
PROV-EV-12.1	Error	“Waiting for Telephony KDC AS Reply”	4000951201	A Kerberos AS Request has been transmitted to the Telephony KDC, but no AS Response has been received.
PROV-EV-13	Error	"Waiting For Telephony KDC TGS Reply"	4000951300	A Kerberos TGS Request has been transmitted to the Telephony KDC, but no TGS Response has been received.
PROV-EV-13.1	Warning	"Telephony KDC did not accept TGS Request"	4000951301	The Telephony KDC rejected the Kerberos TGS Request. (KRB_ERROR)
PROV-EV-14	Critical	"Waiting for CMS AP Reply"	4000951400	A Kerberos AP Request has been transmitted to the CMS (For IPSec), but no AP Response has been received.
PROV-EV-14.1	Warning	"CMS rejected the AP Request (IPSec)"	4000951401	The CMS rejected the Kerberos AP Request. (KRB_ERROR)
PROV-EV-15	Informational	"Provisioning Complete"	4000951500	The MTA successfully completed Provisioning.
PROV-EV-15.1	Warning	"Provisioning Complete - Warnings"	4000951501	The MTA successfully completed Provisioning, but with warnings.
PROV-EV-15.2	Critical	"Provisioning Complete - Fail"	4000951502	The MTA completed Provisioning, but there was a failure.

Event Name	Default Severity for Event	Default Display String	IPCablecom EventID	Comments
PROV-EV-16	Error	“DHCP ERROR: <dhcp-message>;<dhcp-state>[; <error-info>] [;<ip-address-list>]” Note: See Section 7.2 for the normative ABNF, description and requirements.	4000951600	This event indicates the DHCP errors which may occur during the eMTA IPv4 address acquisition process.

Appendix B IPCablecom-defined Powering Events

Note: For sake of simplicity and continuity Event IDs from 4000850100 – 4000950099 are reserved for Powering Events.

MTAs that comply with [5] MUST support the following Powering events.

All Powering events MUST be defined as a matched pair of "set" and "cleared" events. The eight Powering events may be redefined to support a meaning other than the battery-related meanings defined in this document. If these Powering events are redefined, then the definition of the new meaning and any coordination between systems to support this new meaning is out of the scope of IPCablecom.

The "set" and "clear" events for the alarm signals defined in [6] are summarized below.

Telemetry Signal 1 – AC Fail

- PL-EV-1: active alarm state of telemetry signal 1; default meaning "On Battery" and default severity MINOR
- PL-EV-2: inactive alarm state of telemetry signal 1, default meaning "AC Restored"; PL-EV-2 always clears PL-EV-1

Telemetry Signal 2 – Replace Battery

- PL-EV-3: active alarm state of telemetry signal 2; default meaning "Battery Bad" and default severity MINOR
- PL-EV-4: inactive alarm state of telemetry signal 2; default meaning "Battery Good"; PL-EV-4 always clears PL-EV-3

Telemetry Signal 3 - Battery Missing

- PL-EV-5: active alarm state of telemetry signal 3; default meaning "Battery Missing" and default severity MINOR
- PL-EV-6: inactive alarm state of telemetry signal 3; default meaning "Battery Present"; PL-EV-6 always clears PL-EV-5

Telemetry Signal 4 - LowBattery

- PL-EV-7: active alarm state of telemetry signal 4; default meaning "Depleted Battery" and default severity MINOR
- PL-EV-8: inactive alarm state of telemetry signal 4; default meaning "Battery Charging"; PL-EV-8 always clears PL-EV-7

Table 5 - Powering Events

Event Name	Default Severity	Default Display String	IPCablecom EventID	Comments	Associated Events
PL-EV-1	Informational	"On Battery"	4000850100	The UPS has detected an AC power failure and is operating off battery backup.	PL-EV-2
PL-EV-2	Informational	"AC Restored"	4000850200	The UPS has detected AC power restoral and is no longer operating off battery backup.	PL-EV-1
PL-EV-3	Informational	"Battery Bad"	4000850300	The UPS has determined that the battery has reached the end of its life expectancy and should be replaced.	PL-EV-4

Event Name	Default Severity	Default Display String	IPCablecom EventID	Comments	Associated Events
PL-EV-4	Informational	"Battery Good"	4000850400	The UPS has detected the battery to be good.	PL-EV-3
PL-EV-5	Informational	"Battery Missing"	4000850500	The UPS does not detect the presence of a battery.	PL-EV-6
PL-EV-6	Informational	"Battery Present"	4000850600	The UPS detects that a battery is present.	PL-EV-5
PL-EV-7	Informational	"Depleted Battery"	4000850700	The UPS has determined that the remaining battery charge is low. There is only enough charge remaining to sustain operation for a short period of time.	PL-EV-8
PL-EV-8	Informational	"Battery Charging"	4000850800	The UPS detects that the battery has charged above the "battery low" threshold.	PL-EV-7

Appendix C PacketCable-defined Diagnostic Events

Note: For sake of simplicity and continuity Event IDs from 3,000,000,000 to 3,100,000,000 are reserved for diagnostic Events.

Event Name	Default Severity	Default Display String	PacketCable Event ID	Comments
DIAG-EV-1	Critical	"MEM-CONN-ERROR [;<error-info>]" Note: See Section 7.2 for the normative ABNF, description and requirements.	3000000001	This event is created when an eMTA encounters a situation where NV-Events (see Section 7.7) occurred but could not be transmitted due to connectivity errors. See Section 7.6 for more information.
DIAG-EV-2	Critical	"MTA RESET: <reset-reason>:<max-number-of-events-stored>[;<error-info>]" Note: See Section 7.2 for the normative ABNF, description and requirements.	3000000002	This event is created each time the eMTA encounters a hard reboot or a soft reset. It also indicates the associated reason.
DIAG-EV-3	Critical	"ENDPT-HW-ERROR [;<error-info>]" Note: See Section 7.2 for the normative ABNF, description and requirements.	3000000003	This event is created anytime the eMTA encounters a malfunction in the endpoint hardware. For example, due to the physical limitation on REN, or RJ-11 wires are shortened.
DIAG-EV-4	Error	"DOCSIS-CONN-ERROR [;<error-info>]" Note: See Section 7.2 for the normative ABNF, description and requirements.	3000000004	This event is created each time the eMTA encounters the loss of DOCSIS connectivity, for example, due to the T3/T4 timeouts or DOCSIS service flow deletion.