International Telecommunication Union

# ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

# J.172

(11/2005)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

## IPCablecom management event mechanism

ITU-T Recommendation J.172

# ITU-T Recommendation J.172

## IPCablecom management event mechanism

### Summary

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

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

A goal of IPCablecom is to maintain consistency with the Cable Modem event-reporting mechanisms.

### Source

ITU-T Recommendation J.172 was approved on 29 November 2005 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

## CONTENTS

# ITU-T Recommendation J.172

## IPCablecom management event mechanism

### 1 Scope

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

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

A goal of IPCablecom is to maintain consistency with the Cable Modem event-reporting mechanisms.

### 2 References

### 2.1 Normative references

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- ITU-T Recommendation J.164 (2005), *Event message requirements for the support of real-time services over cable television networks using cable modems*.
- ITU-T Recommendation J.166 (2005), *IPCablecom Management Information Base (MIB) framework*.
- ITU-T Recommendation J.167 (2005), *Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems*.
- ITU-T Recommendation M.3100 (2005), *Generic network information model*.
- ITU-T Recommendation X.733 (1992), *Information technology – Open Systems Interconnection – Systems Management: Alarm reporting function*.
- IEFT RFC 3164 (2001), *The BSD syslog Protocol.*

### 2.2 Informative references

- ITU-T Recommendation J.160 (2005), *Architectural framework for the delivery of time-critical services over cable television networks using cable modems*.
- ITU-T Recommendation J.168 (2001), *IPCablecom Media Terminal Adapter (MTA) MIB requirements*.
- IETF RFC 2573 (1999), *SNMP Applications*.
- IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces*.
- ANSI/SCTE 23-3-2003, *DOCSIS 1.1 Part 3: Operations Support System Interface*.

## 3 Terms and Definitions

This Recommendation defines no new terms.

## 4 Abbreviations, acronyms and conventions

### 4.1 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms.

| | |
|---|---|
| CMS | Call Management Server |
| CMTS | Cable Modem Termination System |
| FQDN | Fully Qualified Domain Name (Refer to IETF RFC 821 for details.) |
| IANA | Internet Assigned Numbers Authority |
| MAC | Media Access Control |
| MGC | Media Gateway Controller |
| MIB | Management Information Base |
| MTA | Media Terminal Adapter |
| OSS | Operations Support System |
| SNMP | Simple Network Management Protocol |
| UDP | User Datagram Protocol |

### 4.2 Conventions

If this Recommendation is implemented, the keywords "MUST" and "SHALL" as well as "REQUIRED" are to be interpreted as indicating a mandatory aspect of this Recommendation.

The keywords indicating a certain level of significance of a particular requirement that are used throughout this Recommendation are summarized below:

"MUST" This word or the adjective "REQUIRED" means that the item is an absolute requirement of this Recommendation.

"MUST NOT" This phrase means that the item is an absolute prohibition of this Recommendation.

"SHOULD" This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

"SHOULD NOT" This phrase means that there may exist valid reasons in particular circumstances when the listed behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

"MAY" This word or the adjective "OPTIONAL" means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example, another vendor may omit the same item.

## 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 ITU-T Rec. J.160.

The OSS back office contains business, service, and network management components supporting the core business processes.

The IPCablecom set of Recommendations defines a limited set of OSS functional components and interfaces to support MTA device provisioning, Event Messaging to carry billing information, and the Management Event Mechanism defined in this Recommendation to carry fault and other data.

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

- *ITU-T Rec. J.164 IPCablecom event messages*. This reporting mechanism uses the RADIUS transport protocol, a predefined 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 Cable Modem 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 Recommendation.

## 6 IPCablecom management event mechanism functional requirements

The functional requirements addressed by the message event mechanism Recommendation are as follows:

1) The event report MUST provide either the FQDN or IP address of the reporting device.

   NOTE 1 – It is highly recommended that the device provide the FQDN.

2) The IPCablecom management event reporting mechanism MUST support two types of events: IPCablecom-specific and vendor-specific.

3) The management event reporting mechanism MUST support the IPCablecom Management Event MIB (Annex D/J.166). 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 per RFC 3164.

5) The management event reporting mechanism MUST support SNMPv3/v2c TRAPS, SNMPv3/v2c INFORMS.

6) The management event reporting mechanism MUST comply with SNMP Applications (RFC 3413) 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.

   NOTE 2 – Refer to the IPCablecom MTA Device Provisioning Recommendation (ITU-T Rec. J.167) 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.

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 IPCablecom 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 Mechanism 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 Recommendation and referenced by concerned specifications whereas vendor-specific events are left to vendor implementation and are out of the scope of this Recommendation.

Each Event has an associated Event ID as described in the next clause. IPCablecom-Specific events are identical if their EventIDs are identical. The IPCablecom-Specific EventIDs are specified by the IPCablecom Recommendations, including this Recommendation. 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 are beyond the scope of this Recommendation.

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 Recommendation, event recording MUST conform to the requirements of Annex D/J.166 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 0x800000000 (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 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.

## 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 7.2.

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 ITU-T Rec. J.167. This event data MUST follow the event data format as defined in 7.2.

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 7.2.

Any notification MUST be generated according to the entries in the associated SNMPv3 tables described in IETF 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 Recommendations. Not all IPCablecom Recommendations define management events. Each management event described in the appendix of an IPCablecom Recommendation is assigned an IPCablecom Event ID. For a complete list of IPCablecom Event IDs, refer to 7.1.

### 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 Rec. M.3100 and OSI System Management Alarm Reporting Function (ITU-T Rec. X.733). IPCablecom expands on the definitions 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. Cable Modem, 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 cable operators 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.

## 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 Management Event MIB. 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 Annex D/J.166 provides relative ordering of events in the log. The creation of local volatile and local-non-volatile 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 of the MIB objects in Annex D/J.166 MUST clear both the local-volatile and local-non-volatile logs.

## 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 (RFC 3164).
- It SHOULD use port 514 as the source port, as recommended in section 2 of SNMP applications (RFC 3164).
- It MUST comply with the Packet Format and Contents as defined in section 4 of RFC 3164 as applicable to the origination of the message and use the format as described in the following clause.

### 7.8.1 Syslog message format

This clause defines the usage of the Syslog fields as defined in section 4 of RFC 3164.

### 7.8.2 PRI part of a Syslog packet

For the PRI part defined in 4.1.1 (RFC 3164) 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 4.1 (RFC 3164) 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 ITU-T Rec. J.167 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:
  - IPCABLECOM for all IPCablecom defined Event Messages.
  - A vendor-specific unique identifier for vendor-defined Event Messages. While the vendor-specific choices are out of the scope of this Recommendation, 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 be the correlation ID generated by the MTA as defined in 5.4.5/J.167.
  - Description MUST be the description associated for the particular event as stored in the Management Event MIB (Annex D/J.166).

**Example 1**:

PROV-EV-1 is an IPCablecom defined 'Event', defined as follows:

**Table 1/J.172 – 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 7.8 for more information on turning on SYSLOG messages):

- The Event Priority for critical is 2 (refer to Annex D/J.166 for more information) and hence the 'Priority Code' is 130.
- Since this is an IPCablecom defined event, the 'Event Type Identifier' is 'IPCABLECOM'.
- The defined Event ID is 4000967295 and assuming the default string has not been changed, the associated text is 'Waiting for DNS Resolution of Provisioning Realm Name'.

- 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[IPCABLECOM]:<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/J.172 – 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 ITU-T Recs J.167 and J.166 for more information on turning on SYSLOG messages):

- The Event Priority for warning is 4 (refer to Annex D/J.166 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 IPCablecom 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 another to specify a time period over which those events are generated. The default frequency is defined as 2 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 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 IPCablecom element reboots.

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

### 7.9.1 Severity and priority definition

**7.9.1.1** **Severity** is the degree of failure related to a specific event by a reporting device. Three degrees of severity are commonly used:

- Critical – Used to indicate that 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.

**7.9.1.2** **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. 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 IPCablecom management event data template

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

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 to the appendix of an IPCablecom Recommendation.

Table 3/J.172 – 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 | informational | "MTA Missing Name" | The MTA was not provisioned with an FQDN. | none |

# Annex A

# IPCablecom-defined provisioning events

NOTE – For sake of simplicity and continuity, Event IDs from 4000950100 upwards are reserved for Provisioning Events.

Table A.1/J.172 – Provisioning events

| Event name | Default severity for event | Default display string | Packet-cable 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-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. |

**Table A.1/J.172 – Provisioning events**

| Event name | Default severity for event | Default display string | Packet-cable EventID | Comments |
|---|---|---|---|---|
| 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 | 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-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) |
| 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) SNMPv3 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) SNMPv2c 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. |

### Table A.1/J.172 – Provisioning events

| Event name | Default severity for event | Default display string | Packet-cable EventID | Comments |
|---|---|---|---|---|
| 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. |
| 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) |

**Table A.1/J.172 – Provisioning events**

| Event name | Default severity for event | Default display string | Packet-cable EventID | Comments |
|---|---|---|---|---|
| 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. |

# Annex B

## IPCablecom-defined powering events

NOTE – For the sake of simplicity and continuity, Event IDs from 4000850100-4000950099 are reserved for Powering Events.

MTAs that comply with ITU-T Rec. J.173 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 Recommendation. 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 ANSI/SCTE 23-3-2003 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 B.1/J.172 – 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 |
| 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 |

## SERIES OF ITU-T RECOMMENDATIONS

| | |
|---|---|
| Series A | Organization of the work of ITU-T |
| Series D | General tariff principles |
| Series E | Overall network operation, telephone service, service operation and human factors |
| Series F | Non-telephone telecommunication services |
| Series G | Transmission systems and media, digital systems and networks |
| Series H | Audiovisual and multimedia systems |
| Series I | Integrated services digital network |
| **Series J** | **Cable networks and transmission of television, sound programme and other multimedia signals** |
| Series K | Protection against interference |
| Series L | Construction, installation and protection of cables and other elements of outside plant |
| Series M | Telecommunication management, including TMN and network maintenance |
| Series N | Maintenance: international sound programme and television transmission circuits |
| Series O | Specifications of measuring equipment |
| Series P | Telephone transmission quality, telephone installations, local line networks |
| Series Q | Switching and signalling |
| Series R | Telegraph transmission |
| Series S | Telegraph services terminal equipment |
| Series T | Terminals for telematic services |
| Series U | Telegraph switching |
| Series V | Data communication over the telephone network |
| Series X | Data networks, open system communications and security |
| Series Y | Global information infrastructure, Internet protocol aspects and next-generation networks |
| Series Z | Languages and general software aspects for telecommunication systems |

Printed in Switzerland
Geneva, 2006