

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.370

(06/2008)

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

IPCablecom

IPCablecom2 embedded user equipment provisioning data model specification

Recommendation ITU-T J.370

Downloaded from IHS Markit

Recommendation ITU-T J.370

IPCablecom2 embedded user equipment provisioning data model specification

Summary

Recommendation ITU-T J.370 presents the data element definitions and associated requirements for use with the IPCablecom2 embedded user equipment (E-UE) Provisioning Framework. Specifically, it defines data to be used for configuration and management of E-UEs, and associated users.

Source

Recommendation ITU-T J.370 was approved on 13 June 2008 by ITU-T Study Group 9 (2005-2008) under Recommendation ITU-T A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2009

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
2.1	Normative References	1
2.2	Informative References	2
2.3	Reference Acquisition	2
3	Terms and Definitions	2
4	Abbreviations, acronyms and conventions	3
4.1	Abbreviations and Acronyms	3
4.2	Conventions.....	3
5	Technical Overview.....	3
5.1	Embedded User Equipment (E-UE)	4
5.2	E-UE Provisioning Framework	4
5.3	E-UE Provisioning Data Model.....	4
6	E-UE Provisioning MIBs Framework Requirements	5
6.1	eCM MIB Requirements	6
6.3	Configuration Data Element Requirements.....	10
6.4	Management Event Reporting Requirements.....	11
	Annex A – IPCablecom eUE Common Modules	12
A.1	Textual Conventions MIB Module.....	12
	Annex B – IPCablecom eUE Device Configuration Modules.....	18
B.1	Device Configuration MIB Module	18
B.2	User Configuration MIB Module	29
	Annex C – IPCablecom eUE Provisioning and Management Modules	40
C.1	Provisioning and Management MIB Module	40
C.2	Management Event MIB Module	46
	Annex D – IPCablecom eUE Additional Modules	49
D.1	Certificate Bootstrapping XML Schema	49
	Appendix I – Illustrative IPCablecom Deployment Examples	51
I.1	Example 1: Deployment with multiple Users, and one IPCablecom Application	51
I.2	Example 2: Deployment with multiple Users, and multiple IPCablecom Applications.....	52

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

Recommendation ITU-T J.370

IPCablecom2 embedded user equipment provisioning data model specification

1 Scope

This Recommendation presents the data element definitions and associated requirements for use with the IPCablecom2 E-UE Provisioning Framework. Specifically, it defines data to be used for configuration and management of E-UEs, and associated users. For more information on the IPCablecom2 E-UE Provisioning Framework, please refer to [PKT-EUE-PROV].

This Recommendation does not consider IPCablecom2 application specific data within its scope. IPCablecom2 application specifications are expected to specify such data.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

NOTE – The structure and content of this Recommendation have been organized for ease of use by those familiar with the original source material; as such, the usual style of ITU-T recommendations has not been applied.

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.

[CL-MIB-BB]	Recommendation ITU-T J.199: <i>Battery backup for cable-based devices.</i>
[DOCSIS-RFI]	Recommendation ITU-T J.112: <i>Transmission systems for interactive cable television services.</i>
[eDOCSIS]	Recommendation ITU-T J.126: <i>Embedded Cable Modem device specification.</i>
[PKT-EUE-PROV]	Recommendation ITU-T J.369: <i>IPCablecom2 E-UE Provisioning Specification.</i>
[PKT-SP-PROV1.5]	Recommendation ITU-T J.167: <i>Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems.</i>
[PKT-MEM1.5]	Recommendation ITU-T J.172: <i>IPCablecom management event mechanism.</i>
[RFC2863]	IETF RFC 2863, <i>The Interfaces Group MIB</i> , June 2000.
[RFC3410]	IETF RFC 3410, <i>Introduction and Applicability Statements for Internet Standard Management Framework</i> , December 2002.

- [RFC3412] IETF RFC 3412/STD0062, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*, December 2002.
- [RFC3413] IETF RFC 3413/STD0062, *Simple Network Management Protocol (SNMP) Applications*, December 2002.
- [RFC3414] IETF RFC 3414/STD0062, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*, December 2002.
- [RFC3415] IETF RFC 3415/STD0062, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*, December 2002.
- [RFC3418] IETF RFC 3418, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*.
- [RFC3665] IETF RFC 3665, *Definitions of Managed Objects for the Ethernet-like Interface Types*, September 2003.
- [RFC4113] IETF RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*, June 2005.
- [RFC4293] IETF RFC 4293, *Management Information Base for the Internet Protocol (IP)*, April 2006.
- [IETF STD58] IETF RFC 2578/STD0058, *Structure of Management Information Version 2 (SMIv2)*, April 1999.
- [IETF STD62] IETF RFC 3411/STD0062, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*, December 2002.

2.2 Informative References

This Recommendation uses the following informative reference.

- [ARCH-FRM TR] Recommendation ITU-T J.160: *Architectural framework for the delivery of time-critical services over cable television networks using cable modems*.

2.3 Reference Acquisition

- Internet Engineering Task Force (IETF) Secretariat, 46000 Center Oak Plaza, Sterling, VA 20166, Phone +1-571-434-3500, Fax +1-571-434-3535, <http://www.ietf.org/>.

3 Terms and Definitions

This Recommendation uses the following terms:

3.1 eCM: The logical DOCSIS CM component of a E-UE, complies with DOCSIS, eDOCSIS and IPCablecom requirements.

3.2 eUE: The logical IPCablecom UE component of an E-UE, complies with eSAFE and IPCablecom requirements.

3.3 embedded user equipment (E-UE): A single physical device embedded with an eDOCSIS-compliant DOCSIS Cable Modem and an IPCablecom eUE.

3.4 management information base: The description of the data items used by the Network Management for management and configuration of the IPCablecom compliant E-UE. Such description is done based on the formal meta-language SMI defined by the corresponding IETF standards.

3.5 network management: The functions related to the management of data across the network.

4 Abbreviations, acronyms and conventions

4.1 Abbreviations and Acronyms

This Recommendation uses the following abbreviations:

CM	DOCSIS Cable Modem – a DOCSIS-compliant device which provides data transport connectivity from RFI to IP networks
DOCSIS [®]	Data-Over-Cable Service Interface Specifications
MIB	Management Information Base
OID	Object Identifier. The sequence of integer positive numbers uniquely identifying the position of each MIB Object in the MIB Hierarchy
RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html
SNMP	Simple Network Management Protocol
UDP	User Datagram Protocol. A connectionless protocol built upon Internet Protocol (IP)
VACM	View-based Access Control Model

4.2 Conventions

Throughout this Recommendation, the words that are used to define the significance of particular requirements are capitalized. These words are:

"MUST"	This word 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 means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word 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 Technical Overview

IPCablecom2 is a cable industry specification effort designed to support the convergence of voice, video, data, and mobility technologies. This Recommendation is part of the IPCablecom2 set of specifications and technical reports that define the base architecture and specifies the data elements required to configure and manage E-UEs, associated users and applications, using the IPCablecom2 E-UE Provisioning Framework. For more information about IPCablecom2, please refer to the IPCablecom2 Architecture Framework Technical Report [ARCH-FRM TR]. For more information on the IPCablecom2 E-UE Provisioning Framework, please refer to [PKT-EUE-PROV].

The IPCom2 E-UE Provisioning Framework relies on SNMP, as specified in [IETF STD62], for configuration and management. The data is specified using Structure of Management Information, Version 2 (SMIv2) Management Information Bases (MIBs), as specified in [IETF STD58]. Thus, this Recommendation specifies the configuration and management MIBs for use with the IPCom2 E-UE Provisioning Framework.

In this Recommendation, the term "DOCSIS" is used to refer to DOCSIS version 1.1 or later, unless explicitly specified otherwise. Additionally, all references to IPCom within this Recommendation are assumed to be IPCom2, unless stated otherwise.

5.1 Embedded User Equipment (E-UE)

The E-UE is a single physical device embedded with an eDOCSIS-compliant DOCSIS Cable Modem (eCM) and an eUE that complies with eDOCSIS eSAFE and IPCom UE requirements. For more information on E-UEs please refer to [PKT-EUE-PROV].

5.2 E-UE Provisioning Framework

The E-UE Provisioning Framework is an IPCom2 configuration and management framework based on the IPCom 1.5 Device Provisioning specification. For more information on the E-UE Provisioning Framework, please refer to [PKT-EUE-PROV].

This Recommendation is to be used in conjunction with the E-UE Provisioning Framework, and also relies on the IPCom 1.5 Device Provisioning specification. For more information on the latter, please refer to [PKT-SP-PROV1.5].

5.3 E-UE Provisioning Data Model

The E-UE Provisioning Data Model serves eCMs, eUEs, users and associated applications. For the eCM component it borrows from the DOCSIS suite of specifications with no additional enhancements. The eUE, user and application data are logically separated, and specified in this Recommendation. Given the use of SNMP for configuration and management, the eUE component is provided with data pertaining to itself, users and applications.

The logical representation of the E-UE Provisioning Data Model is specified in Figure 1.

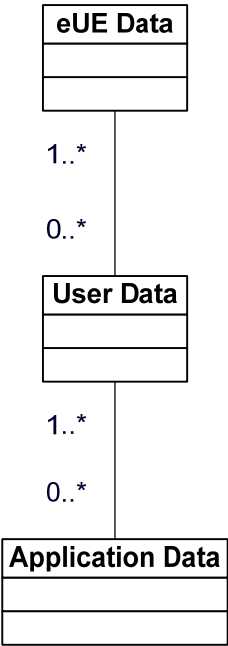


Figure 1 – E-UE Provisioning Data Model

6 E-UE Provisioning MIBs Framework Requirements

The E-UE MIBs framework provides the MIB module implementation requirements for the E-UE. An informative, logical framework depicting MIB modules in the E-UE components is presented in Figure 2. The rest of this clause presents the specific requirements.

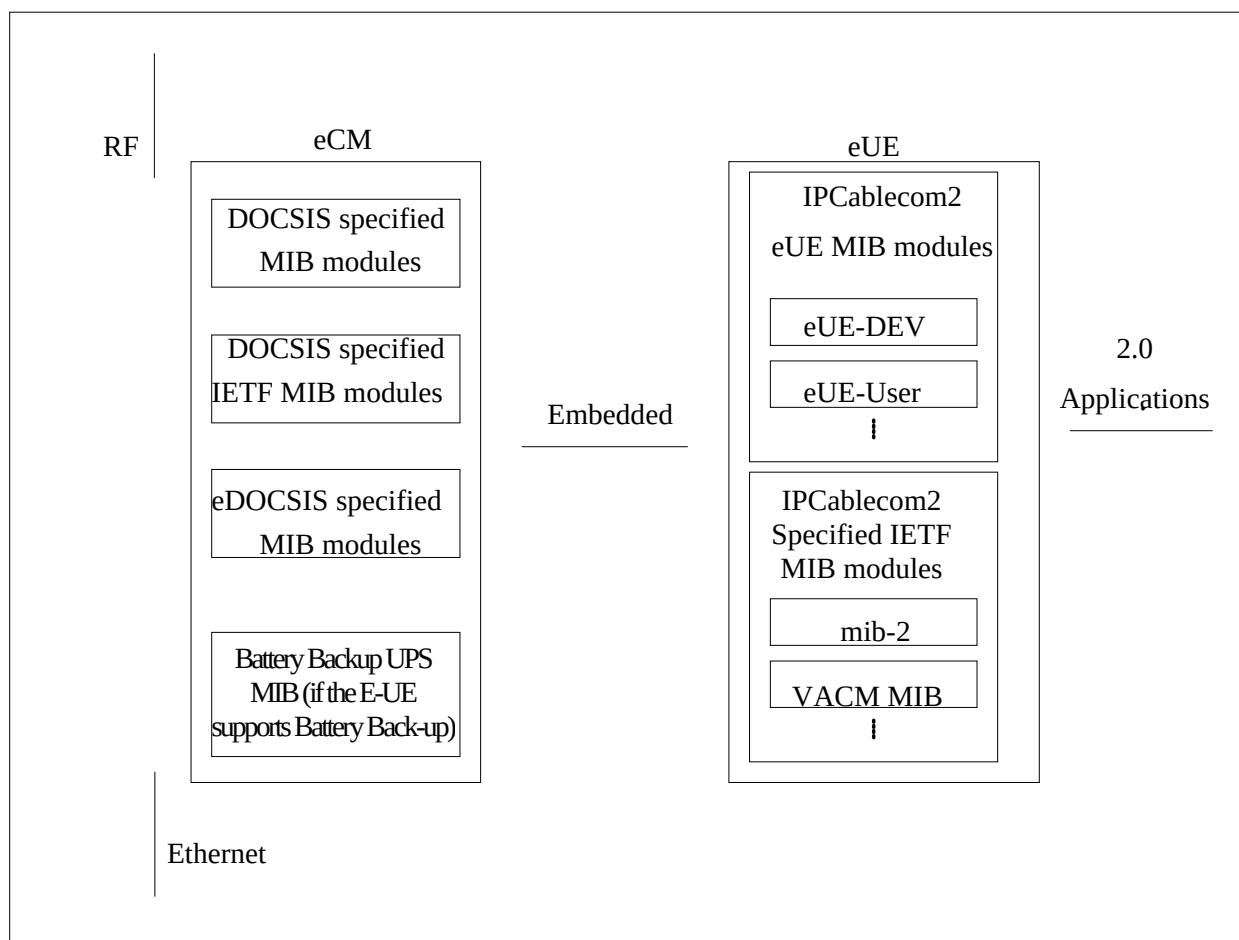


Figure 2 – E-UE Logical MIBs Framework

The eCM component of an E-UE needs to comply with the DOCSIS and eDOCSIS suite of specifications. The eUE component is required to support the data model that was informatively described in clause 5.3. To provide more information:

- The eUE can be associated with one or more Users.
- Each User can be associated with one or more applications.
- Each application has one more features; each feature has a set of configuration data.

Furthermore, each User can be associated with one or more eUEs. However, this is not possible to achieve using an SNMP-based framework that requires the data to be physically stored on a single client. In the E-UE Provisioning framework, this client is the eUE (for IPCablecom data). Support for the other requirements is achieved by using an array of mappings:

- Association of an eUE with multiple Users
- Association of a User with multiple Applications; each Application being associated with one Profile

- Association of a Profile with multiple features; some of which could be shared with other Profiles belonging to the same Application

6.1 eCM MIB Requirements

This clause presents the MIB module requirements for the eCM component of the E-UE.

6.1.1 DOCSIS MIB Modules

The eCM component of an E-UE MUST comply with the DOCSIS MIB module requirements. For more information on the DOCSIS MIB modules, please refer to the DOCSIS Recommendations.

6.1.2 eDOCSIS MIB Modules

The eCM component of an E-UE MUST comply with the eDOCSIS MIB requirements. For more information on the eDOCSIS MIB module requirements, please refer to the eDOCSIS Recommendation [eDOCSIS].

6.1.3 Battery Backup UPS MIB module

If the E-UE supports Battery Backup functionality, as specified in [CL-MIB-BB], the eCM component MUST support the Battery Backup and UPS MIB and associated requirements.

6.2 eUE MIB Requirements

This clause presents the MIB module requirements for the eUE component of the E-UE.

6.2.1 eUE MIB Modules

The eUE component of the E-UE MUST comply with the IPCablecom2 specified eUE MIB configuration and management MIB modules specified in Annexes B and C, respectively.

6.2.2 IETF MIB Modules

The eUE MUST implement the following MIB modules:

- MIB II system group as specified in [RFC3418];
- IF MIB as specified in [RFC2863];
- Ethernet MIB as specified in [RFC3665];
- UDP MIB as specified in [RFC4113]; and
- IP MIB as specified in [RFC4293].

6.2.3 SNMP MIB Requirements

6.2.3.1 eUEsysDescr Requirements

The eUE's MIB II sysDescr MIB object MUST conform to the format specified in the DOCSIS specifications governing the eCM component.

6.2.3.2 eUE ifTable Requirements

The eUE MUST implement the row entry specified in Table 1 for the ifTable as specified in [RFC2863].

Table 1 – eUE ifTable Requirements

ifTable ([RFC2863])	Row Entry
IfIndex	1
ifDescr	"DOCSIS Embedded Interface"
IfType	other(1)
IfMtu	0
IfSpeed	0
ifPhysAddress	eUE MAC address
IfAdminStatus	up(1)
ifOperStatus	up(1)
IfLastChange	per [RFC2863]
ifInOctets (optional)	(n) if implemented, else 0
IfInNUCastPkts	Deprecated
IfInDiscards	0
IfInErrors	0
IfUnknownProtos	0
ifOutOctets (optional)	(n) if implemented, else 0
ifOutUCastPkts (optional)	(n) if implemented, else 0
IfOutNUCastPkts	Deprecated
IfOutDiscards	0
IfOutErrors	0
IfOutQlen	Deprecated
IfSpecific	Deprecated

6.2.3.3 eUE ipNetToPhysicalTable Requirements

The eUE MUST implement the row entry specified in Table 2 for the ipNetToPhysicalTable as specified in [RFC4293].

Table 2 – ipNetToPhysicalTable MIB Object Details

ipNetToPhysicalTable	CM device
ipNetToPhysicalIfIndex	1
ipNetToPhysicalPhysAddress	eCM MAC Address
ipNetToPhysicalNetAddressType	ipv4(1) or ipv6(2)
ipNetToPhysicalNetAddress	eCM IP Address
ipNetToPhysicalLastUpdated	<refer to [RFC4293]>
ipNetToPhysicalType	static(4)
ipNetToPhysicalState	<refer to [RFC4293]>
ipNetToPhysicalRowStatus	'active'

6.2.3.4 eUE USM Requirements

This clause presents the IPCablecom2 eUE USM requirements. Please refer to [RFC3414] for more information on the User-based Security Model (USM) for SNMPv3.

An eUE, provisioned in the Secure Provisioning Flow, **MUST** configure the `usmUserTable` immediately after receiving the AP REPLY from the Provisioning Server, with the entry specified in Table 3.

Table 3 – eUE `usmUserTable` Entry

usmUserTable ([RFC3414][IETF STD62])	Row Entry
<code>usmUserEngineID</code>	The SNMP local engine id
<code>usmUserName</code>	eUE-Prov-xx:xx:xx:xx:xx:xx, where xx:xx:xx:xx:xx:xx represents the eUE's Mac address
<code>usmUserSecurityName</code>	eUE-Prov-xx:xx:xx:xx:xx:xx, where xx:xx:xx:xx:xx:xx represents the eUE's Mac address
<code>usmUserCloneFrom</code>	0.0
<code>usmUserAuthProtocol</code>	<code>usmHMACMD5AuthProtocol</code> or <code>usmHMACSHAAuthProtocol</code>
<code>usmUserAuthKeyChange</code>	""
<code>usmUserOwnAuthKeyChange</code>	""
<code>usmUserPrivProtocol</code>	<code>usmDESPrivProtocol</code> if privacy is indicated in AP REPLY <code>usmNoPrivProtocol</code> if privacy is not indicated in the AP REPLY
<code>usmUserPrivKeyChange</code>	""
<code>usmUserOwnPrivKeyChange</code>	""
<code>usmUserPublic</code>	""
<code>usmUserStorageType</code>	volatile
<code>usmUserStatus</code>	active

Initial authentication and privacy keys for this user are derived from the AP Reply message. The eUE **MUST** allow for cloning of users as specified in [IETF STD62]. This can be accomplished using the configuration file, or dynamically through SNMP SET operations.

6.2.3.5 eUE VACM Requirements

This clause presents the IPCablecom2 eUE VACM requirements. For more information regarding View-based Access Control Model (VACM) for SNMP, please refer to [RFC3415].

The eUE **MUST** configure the `VacmSecurityToGroupTable` with the entry specified in Table 4.

Table 4 – eUE `VacmSecurityToGroupTable`

VacmSecurityToGroupTable ([RFC3415])	Row Entry
<code>vacmSecurityModel</code>	USM
<code>vacmSecurityName</code>	eUE-Prov-xx:xx:xx:xx:xx:xx
<code>vacmGroupName</code>	<code>IPCablecomFullAccess</code>
<code>vacmSecurityToGroupStorageType</code>	volatile
<code>vacmSecurityToGroupStatus</code>	active

The eUE MUST configure the vacmAccessTable with the entry specified in Table 5 and the associated requirements that follow. This configuration allows for read access of all MIB modules in the eUE, write access to IPCablecom 2.0 eUE MIB modules, and notifications as specified in the IPCablecom2 eUE MIB modules.

Table 5 – eUE vacmAccessTable

vacmAccessTable (RFC3415)	Row Entry
vacmGroupName	IPCablecomFullAccess
vacmAccessContextPrefix	""
vacmAccessSecurityModel	USM
vacmAccessSecurityLevel	authPriv or authNoPriv (depending on whether privacy has been specified)
vacmAccessContextMatch	exact
vacmAccessReadViewName	ReadOnlyView
vacmAccessWriteViewName	FullAccessView
vacmAccessNotifyViewName	NotifyView
vacmAccessStorageType	volatile
vacmAccessStatus	active

The following requirements are associated with Table 5.

- The eUE's ReadOnlyView MUST consist of the entire MIB tree contained in the eUE.
- The eUE's FullAccessView MUST consist of all the IPCablecom-specified MIB modules, the MIB-II system group, and the IF-MIB tree.
- The eUE's FullAccessView MAY include vendor-specific MIBs, VACM, USM, and Notifications MIB.
- The eUE's NotifyView MUST consist of all the IPCablecom2 specified MIB modules, the MIB-II system group, and the snmpTrapOID MIB tree.
- The eUE's NotifyView MAY include vendor-specific MIB trees.

6.2.3.6 SNMPv2c Management Requirements

The eUE MUST follow the SNMPv2c management requirements as specified in [PKT-SP-PROV1.5], "SNMPV2C MANAGEMENT REQUIREMENTS", with the following clarifications:

- The requirements applicable to the eMTA apply to the eUE.
- The string (or substring) "mta" is replaced with "eue" in snmpCommunityIndex, snmpCommunitySecurityName, snmpCommunityTransportTag, snmpTargetAddrName, snmpTargetAddrTagList, snmpTargetAddrParams, vacmSecurityName, vacmGroupName, VacmAccessReadViewName, VacmAccessWriteViewName, vacmAccessNotifyViewName, vacmViewTreeFamilyViewName, snmpTargetParamsName, snmpTargetParamsSecurityName, snmpNotifyName, snmpNotifyTag, snmpNotifyFilterProfileName and snmpNotifyFilterSubtree.
- Any references to MIB modules, such as pktcMtaNotification within the snmpNotifyFilterTable, applies to the IPCablecom2 E-UE MIB modules.

6.3 Configuration Data Element Requirements

The eCM MUST comply with the DOCSIS and eDOCSIS configuration data element requirements, including mandatory, optional and prohibited MIB Objects. The eUE MUST report any configuration data elements deemed mandatory, and not provided in the respective configuration file.

6.3.1 Configuration File Requirements

This clause provides the configuration data element requirements.

Table 6 – eUE Configuration Data Element Requirements

MIB Module (CL-PKTC-)	Data Element	Requirement	Additional Details
EUE-PROV-MGMT-MIB	pktcMtaDevEnabled	Mandatory	This element is always required.
EUE-PROV-MGMT-MIB	pktcMtaDevRealmOrgName	Conditionally Mandatory	This element is mandatory in the Secure Provisioning Flow.
EUE-DEV-MIB	pktcEUEDevOpTable	Conditionally Mandatory	One table entry is mandatory if the eUE has any active users associated with it.
EUE-DEV-MIB	pktcEUEDevDnsTable	Conditionally Mandatory	One table entry is mandatory if the eUE has any active users associated with it.
EUE-DEV-MIB	pktcEUEDevPCSCFTable	Conditionally Mandatory	One table entry is mandatory if the eUE has any active users associated with it.
EUE-USER-MIB	pktcEUEUsrIMPUPTable	Conditionally Mandatory	One table entry is mandatory if the eUE has any active users associated with it.
EUE-USER-MIB	pktcEUEUsrIMPITable	Conditionally Mandatory	One table entry is mandatory if the eUE has any active users which need authentication for registration.
EUE-USER-MIB	pktcEUEUsrAppMapTable	Conditionally Mandatory	One table entry is mandatory if any active user has any applications associated with it.

6.3.2 Certificate Bootstrapping File Requirements

This clause provides the Certificate Bootstrapping configuration data element requirements.

Table 7 – eUE Configuration Bootstrapping Requirements

XML Schema	Data Element	Requirement	Additional Details
CL-PKTC-CB	pktcEUEClearCurrentCredentials	Mandatory	At least one instance is required
CL-PKTC-CB	pktcEUEUsrIMPIType	Conditionally Mandatory	Required for an instance of an IMPI
CL-PKTC-CB	pktcEUEUsrIMPI	Conditionally Mandatory	Required for an instance of an IMPI
CL-PKTC-CB	pktcEUEUsrIMPICredsType	Conditionally Mandatory	Required for an instance of an IMPI
CL-PKTC-CB	pktcEUEUsrIMPICreds	Conditionally Mandatory	Required for an instance of an IMPI

6.4 Management Event Reporting Requirements

The E-UE MUST support all the Management Events specified in [PKT-MEM1.5], Table 4, except for the following:

- PROV-EV-12
- PROV-EV-12.1
- PROV-EV-13
- PROV-EV-13.1
- PROV-EV-14
- PROV-EV-14.1

In addition, the eUE MUST support the management events specified in Table 8.

Table 8 – Additional eUE Management Events

Event Name	Default Severity for Event	Default Display String	IPCablecom Event ID	Comments
EUE-EV-1	error	"Registration did not comply with SigSecurity configuration for user <user IMPU>"	4000960000	The eUE MUST report this event if the directive specified in pktcEUEUsrIMPUSigSecurity is not met during registration of a user IMPU.
EUE-EV-2	critical	"Registration failed for user IMPU=<user IMPU>; IMPI=<user IMPI>; reason <reason>"	4000960001	The eUE MUST report this event if the registration for a specific user failed. The eUE MUST populate <user IMPU> with the user's IMPU and <user IMPI> with the user's IMPI.
EUE-EV-3	informational	"Certificate Bootstrapping Success"	4000960002	The eUE MUST report this event if a Certificate Bootstrapping procedure that was initiated was successfully completed.
EUE-EV-4	critical	"Certificate Bootstrapping Failure"	4000960003	The eUE MUST report this event if a Certificate Bootstrapping procedure was not successfully completed.

Annex A

IPCablecom eUE Common Modules

(This annex forms an integral part of this Recommendation)

A.1 Textual Conventions MIB Module

```
CL-PKTC-EUE-TC-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32
        FROM SNMPv2-SMI
    MODULE-COMPLIANCE
        FROM SNMPv2-CONF
    TEXTUAL-CONVENTION, TruthValue
        FROM SNMPv2-TC
    SnmpAdminString
        FROM SNMP-FRAMEWORK-MIB
    pktcEUEMibs
        FROM CLAB-DEF-MIB;

pktcEUETCMIB MODULE-IDENTITY
    LAST-UPDATED "200711060000Z"
    ORGANIZATION "Cable Television Laboratories, Inc."
    CONTACT-INFO
        "Sumanth Channabasappa
        Cable Television Laboratories, Inc.
        858 Coal Creek Circle,
        Louisville, CO 80027, USA
        Phone: +1 303-661-9100
        Email: mibs@cablelabs.com

        Acknowledgements:
        Thomas Clack, Broadcom - Primary author,
        and members of the PacketCable PACM Focus Team."
    DESCRIPTION
        "This MIB module specifies the TEXTUAL CONVENTIONS
        for use in the definition of PacketCable E-UE
        MIB Objects."
    ::= { pktcEUEMibs 2 }

-- Administrative assignments
pktcEUETCNotifications OBJECT IDENTIFIER ::= { pktcEUETCMIB 0 }
pktcEUETCObjects OBJECT IDENTIFIER ::= { pktcEUETCMIB 1 }
pktcEUETCConformance OBJECT IDENTIFIER ::= { pktcEUETCMIB 2 }

pktcEUETCCompliances OBJECT IDENTIFIER ::= { pktcEUETCConformance 1 }
pktcEUETCGroups OBJECT IDENTIFIER ::= { pktcEUETCConformance 2 }

-- MIB Objects
pktcEUETCUsageObjs OBJECT IDENTIFIER ::= { pktcEUETCObjects 1 }

-----
-- TEXTUAL CONVENTION for defining EUE Identifiers
-----
PktcEUETCID ::= TEXTUAL-CONVENTION
    STATUS current
    DESCRIPTION
        " This TEXTUAL CONVENTION is being defined
        to contain identities that can be used
        within the PacketCable eUE data models.
```

It specifies a hex string that can be used to represent the various identities.

The types of possible identities are specified by the TEXTUAL CONVENTION 'PktcEUETCIDType'.

The following rules apply:

- All identities, except macaddress refer to either UEs or Users.
Mac addresses are UE specific
- When used as a pair, the public and private identities MUST be separated by a '#', with the private identity following the public identity."

SYNTAX OCTET STRING(SIZE(0..1023))

-- TEXTUAL CONVENTION for defining EUE Identifier type

PktcEUETCIDType ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

" This TEXTUAL CONVENTION is being defined as a way of indicating an identity specified by MIB Objects utilizing the TEXTUAL CONVENTION 'PktcEUETCID'.

The defined types include:

- other(1)
for types not described by the options provided below
- gruu(2)
for Globally Routable Unique URIs
- publicIdentity(3)
for Public Identities as defined by PacketCable
- privateIdentity(4)
for Private Identities as defined by PacketCable
- publicPrivatePair(5)
for Public and Private Identity pairs as defined by PacketCable
- username(6)
for username and password as defined by PacketCable
- macaddress(7)
for mac addresses
- packetcableIdentity(8)
for PacketCable specific types

UE implementations must ensure that PktcEUETCIDType objects and any dependent objects (e.g., PktcEUETCID objects) are consistent.

In general, the UE MUST generate an 'inconsistentValue' error if an attempt to change an PktcEUETCIDType object would, for example, lead to an undefined PktcEUETCID value.

In particular, PktcEUETCIDType/PktcEUEID pairs MUST be changed together."

SYNTAX INTEGER {
 other(1),
 gruu(2),
 publicIdentity(3),
 privateIdentity(4),
 publicPrivatePair(5),
 username(6),
 macaddress(7),
 packetcableIdentity(8)
}