International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.369

(06/2008)

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

IPCablecom

IPCablecom2 E-UE provisioning framework specification

Recommendation ITU-T J.369

Recommendation ITU-T J.369

IPCablecom2 E-UE provisioning framework specification

Summary

Recommendation ITU-T J.369 specifies the network and protocol requirements to configure and manage IPCablecom2 Embedded User Equipment (E-UE) along with the associated users and applications.

Source

Recommendation ITU-T J.369 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/.

CONTENTS

Recommendation ITU-T J.369

IPCablecom2 E-UE provisioning framework specification

1 Scope

This Recommendation describes the provisioning mechanism for IPCablecom2 Embedded User Equipment (E-UE). The purpose is to specify the network and protocol requirements to configure and manage E-UEs, along with the associated users and applications. The configuration and management data requirements are specified in a related document, the E-UE Provisioning Data Models Specification [PKT-EUE-DATA].

The configuration and management of non-embedded UEs such as software-based clients, and network elements such as the CSCFs and the HSS, is out of scope for this Recommendation.

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-BB-MIB] Recommendation ITU-T J.199: *Battery backup for cable-based devices*.

[CL-CANN-DHCP-Reg] Recommendation ITU-T J.166: *IPCablecom Management Information Base (MIB) framework Annex A.*

[DOCSIS-RFI] Recommendation ITU-T J.112: *Transmission systems for interactive cable television services.*

[eDOCSIS] Recommendation ITU-T J.126: *Embedded Cable Modem device specification.*

[PKT-PROV1.5] Recommendation ITU-T J.167: *Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems*.

[PKT-SEC1.5] Recommendation ITU-T J.170: *IPCablecom security specification.*

[PKT-MEM1.5] Recommendation ITU-T J.172: *IPCablecom management event mechanism.*

[PKT-EUE-DATA] Recommendation ITU-T J.370: *IPCablecom2 Provisioning data model Specification*.

[RFC 1034] RFC1034/STD0013, *Domain names – concepts and facilities, November 1987*.

[RFC 1035] RFC1035/STD0013, *Domain names – implementation and specification, November 1987*.

[RFC 1350] IETF RFC 1350/STD0033, *The TFTP protocol (Revision 2), July 2003*.

[RFC 2131] IETF RFC 2131, *DHCP*: *Dynamic Host Configuration Protocol, March 1997*.

[RFC 2234] IETF RFC 2234, *Augmented BNF for Syntax Specifications: ABNF, November 1997*.

[RFC 2246] IETF RFC 2246, *The TLS Protocol Version 1.0, January 1999*.

[RFC 2461] IETF RFC 2461, *Neighbor Discovery for IP Version 6 (IPv6), December 1998*.

[RFC 2462] IETF RFC 2462, *IPv6 Stateless Address Autoconfiguration, December 1998*.

[RFC 2616] IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1, June 1999*.

[RFC 2782] IETF RFC 2782, *A DNS RR for specifying the location of services (DNS SRV), February 2000*.

[RFC 2915] IETF RFC 2915, *The Naming Authority Pointer (NAPTR) DNS Resource Record, September 2000.*

[RFC 3164] IETF RFC 3164, *BSD Syslog protocol, August 2001*.

[RFC 3268] IETF RFC 3268, *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002*.

[RFC 3315] IETF RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003*.

[RFC 3396] IETF RFC 3396, *Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4), November 2002*.

[RFC 3411] IETF RFC 3411/STD0062, *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks.*

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

[RFC 3414] IETF RFC 3414/STD0062, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002*.

[RFC 3495] IETF RFC 3495, *Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration, March 2003.*

[RFC 3513] IETF RFC 3513, *Internet Protocol Version 6 (IPv6) Addressing Architecture, April 2003*.

[RFC 3584] IETF RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, August 2003*.

[RFC 3594] IETF RFC 3594, *PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option, September 2003*.

[RFC 3596] IETF RFC 3596, *DNS Extensions to Support IP Version 6, October 2003.*

[RFC 3617] IETF RFC 3617, *Uniform Resource Identifier (URI) Scheme and Applicability Statement for the Trivial File Transfer Protocol (TFTP), October 2003.*

[RFC 3925] IETF RFC 3925, *Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4), October 2004.*

[RFC 4291] IETF RFC 4291, *IP Version 6 Addressing Architecture, February 2006.*

[RFC 4361] IETF RFC 4361, *Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4). February, 2006.*

[RFC 4704] IETF RFC 4704, *The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client, October 2006.*

2.2 Informative references

This Recommendation uses the following informative references.

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

[PKT-24.229] Recommendation ITU-T J.366.4 (draft): *IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification.*

[RFC 3319] IETF RFC 3319, *H. Schulzrinne, B. Volz, Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers, July 2003.*

2.3 Reference acquisition

- Cable Television Laboratories, Inc., 858 Coal Creek Circle, Louisville, CO 80027; Phone +1-303-661-9100; Fax +1-303-661-9199; http://www.cablelabs.com.
- 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 defines the following terms:

3.1 configuration: Configuration is the process of defining and propagating data to network elements for providing services.

3.2 data model: An abstract model that describes representation of data in a system.

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

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

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

3.6 **Kerberos**: Authentication protocol allowing one network entity (Client) to be mutually authenticated to another one (Application Server) using the "Kerberos ticket" retrieved by the Client from a dedicated Authentication Server (KDC).

3.7 **provisioning**: Provisioning refers to the processes involved in the initialization of user attributes and resources to provide services to a User. This involves protocols, methodologies, and interfaces to network elements such as: Order Entry and Workflow Systems that carry out business processes, Operational Support Elements that handle network resources, Application Servers that offer services and User Equipment that offer services, among others.

4 Abbreviations, acronyms and conventions

4.1 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

CODEC	COding-DECoding algorithms used to compress/decompress the data representing the Voice (or Video) media traffic
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HTTP	HyperText Transfer Protocol
KDC	Key Distribution Center: the Authentication Server which implements the Kerberos PKINIT Authentication Protocol
MIB	Management Information Base
MSO	Multiple System Operator (A network operator)
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SYSLOG	System Logging Protocol – a protocol which defines the transport mechanism for the messages carrying various logging information
TFTP	Trivial File Transfer Protocol
TGT	Ticket Granting Ticket
ToD	Time of the Day – the network protocol which delivers the time of the day to a network client from the Time Of the Day from the network server
UE	User Equipment

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 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 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

The framework specified for configuration and management in this Recommendation reuses the protocols and interfaces specified for Embedded Multimedia Terminal Adaptors (E-MTAs) in the IPCablecom Device Provisioning specification [PKT-PROV1.5]. As such, this Recommendation presents a specific profile of the IPCablecom Device Provisioning solution. In addition, it enhances device provisioning to address additional requirements that are in scope for eUEs, but not eMTAs. Specifically, eUEs connect to the IPCablecom architecture based on SIP and the IMS, and support IPv6. The following subclauses provide more details on E-UEs, the reuse of Device Provisioning, and related aspects.

5.1 Embedded User Equipment (E-UE)

IPCablecom is based on SIP and IMS, and aims to support a wide variety of clients such as embedded eDOCSIS clients (e.g., telephony devices), non-embedded clients (e.g., dual-mode handsets), and software-based clients. Consistent with the IMS, IPCablecom clients are termed User Equipment (UE). For more information about UEs in IPCablecom, please refer to the IPCablecom Architecture Framework Technical Report ([PKT-ARCH-TR]).

This Recommendation considers only one family of UEs – those embedded with a DOCSIS Cable Modem, termed E-UE. Specifically, 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 IPCablecom UE requirements. Consistent with eDOCSIS terminology, the logical DOCSIS and UE components are referenced by the terms eCM and eUE, respectively. For more information about eDOCSIS, please refer to the eDOCSIS specification ([eDOCSIS]).

It is to be noted that the term "DOCSIS" in this Recommendation is understood to refer to DOCSIS version 1.1 or later unless explicitly stated otherwise. Please refer to the corresponding DOCSIS specifications for more information about DOCSIS (for instance, DOCSIS 1.1 is specified in [DOCSIS-RFI] and associated specifications).

5.2 Provisioning

Provisioning refers to the processes involved in the initialization of the attributes and resources on clients and network components to provide services to a user. The term Provisioning, in this Recommendation, refers to the process of configuration and readiness for management of E-UEs. Configuration is generally specified as the process of defining and transporting the provisioning data to the network elements providing services. Management refers to the protocols, methodologies and interfaces that enable monitoring, and the control and availability of the offered services in an Operator's Network.

5.3 Reuse of IPCablecom Device Provisioning

IPCablecom Device Provisioning is a configuration and management solution designed for embedded IPCablecom devices, specifically the IPCablecom Embedded Multimedia Terminal Adaptors (E-MTAs). It is based on IETF standards and protocols such as SNMP ([RFC3411]),

DHCP ([RFC2131]), and TFTP ([RFC1350]). This is currently being used by network operators for IPCablecom deployments.

To reuse the existing OSS infrastructure and to expedite roll out of E-UEs with minimal OSS changes, this Recommendation offers a framework that reuses the protocols and interfaces specified by IPCablecom Device Provisioning with enhancements to support IPCablecom E-UEs. The enhancements include:

- Support for IPv6 eUEs.
- Support for eUEs connecting to an IPCablecom network.

To minimize the restating of requirements, this Recommendation makes numerous references to [PKT-PROV1.5], with the following clarifications.

- All requirements regarding Telephony Services are not applicable and will be ignored.
- Any IPCablecom Signalling requirements (e.g., endpoint provisioning for CMSs), are not applicable to eUEs.
- Requirements for the E-MTA or eMTA will be interpreted as requirements for E-UE and eUE, respectively, in referenced clauses.
- All references to data definitions, such as the MTA MIB, will be interpreted in accordance with [PKT-EUE-DATA] and explicit data requirements in this Recommendation.
- For any conflict in requirements, this Recommendation will always take precedence over [PKT-PROV1.5].

5.4 IP Network Environments

Given their embedded nature, E-UEs will always connect via a DOCSIS network. Thus, the DOCSIS Operator controls the IP network connectivity and IP parameters such as IP address information. Further, IPCablecom supports E-UEs that can be IPv4, IPv6, or both. This Recommendation allows for the specified IP network versions, and allows for a choice between IPv4 and IPv6 for the eUE when the eCM is provisioned. This is an enhancement for IPCablecom Device Provisioning, which only handles IPv4 eSAFE clients.

5.5 E-UE Provisioning Model

E-UE Provisioning supports static and dynamic configuration of E-UEs. Static configuration is specified as a pre-established set of configuration parameters for an E-UE that is pre-configured in the Operator's network. In contrast, dynamic configuration is characterized by the capability to create and provide configuration to E-UEs dynamically, even those that are not pre-configured in the Operator's network. Dynamic provisioning can be used to provide emergency or subscription-related information such as emergency dialing for voice services and self-subscription redirects. It is to be noted that support for dynamic configuration during any particular deployment is a choice left to the network operator.

The eCM component of an E-UE is governed by the DOCSIS specifications and any enhancements provided explicitly in this Recommendation, such as IPCablecom-specific DHCP options. The provisioning of the eUE is accomplished using the provisioning flows specified in this Recommendation. There are three kinds of eUE flows: Basic, Hybrid and Secure. A provisioning flow is selected when the eUE initializes and obtains its IP configuration information. The provisioning flow is deemed complete when the eUE obtains its configuration via a configuration file.

A high-level conceptual diagram highlighting all the components and the provisioning flows is indicated in Figure 1.

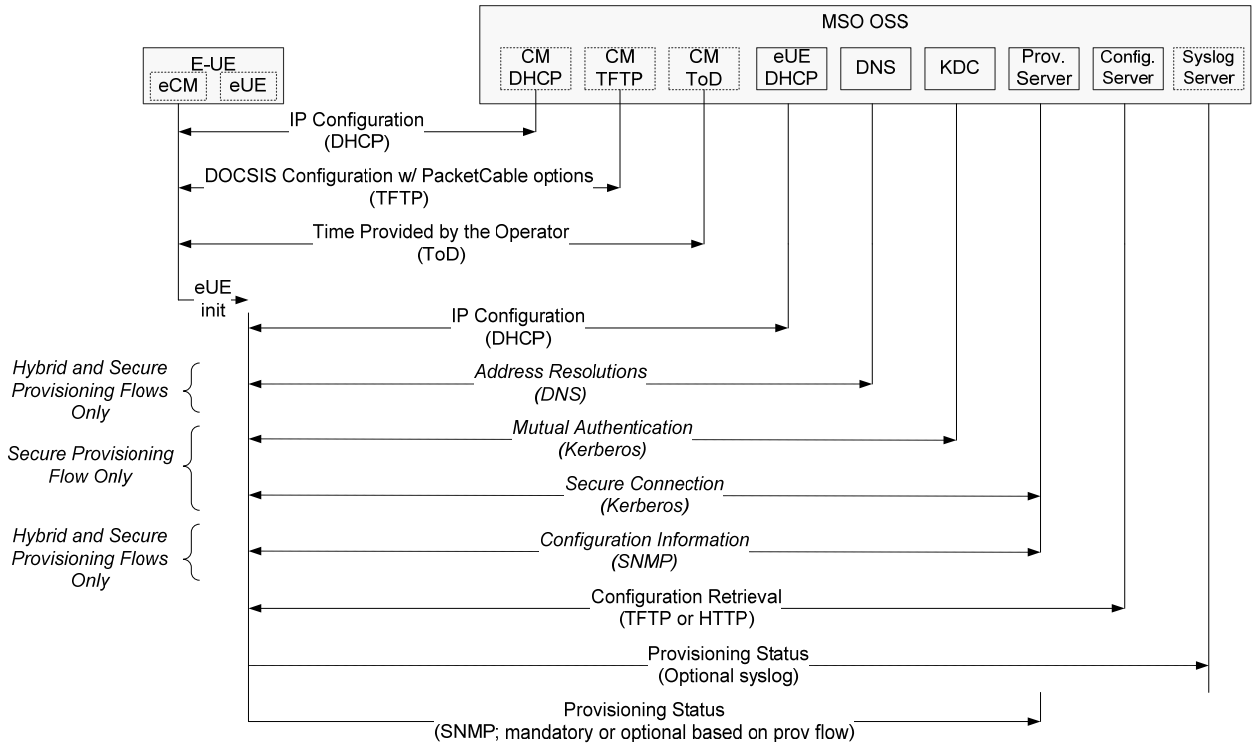

Figure 1 – IPCablecom E-UE Provisioning Flow (conceptual)

As indicated in Figure 1, the reset of an E-UE results in the eCM component being initialized first. Once the eCM has been provisioned, and if it obtains IPCablecom-specific parameters, the eUE is initialized. The eUE is then provided with IP configuration information that indicates the choice of provisioning flow.

Figure 1 also highlights various OSS components required for eUE provisioning. Their roles can be briefly summarized as follows:

DHCP Server

The DHCP server is used in all the provisioning flows and provides IP configuration information, such as the IP address and DNS server information. In addition, it is also used to provide IPCablecom-specific configuration, such as the choice of provisioning flow and network component information (e.g., Kerberos realm in the secure provisioning flow).

DNS Server

The DNS server is primarily used in the Hybrid and Secure provisioning flows and allows the eUE to discover the IP address of network components, such as the KDC and the Provisioning Server. The DNS server itself is obtained via DHCP as part of the IP configuration information.

KDC

The KDC is the authentication server specified by the Kerberos protocol. It is used for mutual authentication between the eUE and the network operator's network. It also facilitates mutual authentication between the E-UE and the Provisioning server, and with SNMPv3 connectivity establishment in the case of the secure provisioning flow.

Provisioning Server

The Provisioning Server containing the SNMP entity is used in the Hybrid and Secure provisioning flows to provide configuration to the eUE. In the case of the secure provisioning flow, this component also acts as a Kerberos Application Process.

It uses SNMP for configuration in the Hybrid and Secure Provisioning flows. In the secure mode, SNMPv3 is used to exchange authentication, and optional encryption, information related to the configuration file.

TFTP and HTTP Servers

TFTP and, optionally, HTTP servers can be used to propagate the configuration file to the eUE.

Syslog Server

Syslog Servers are used to collect management events from the client. To use syslog, the eUE needs to be configured with a valid Syslog Server and syslog enabled as a management event transport.

5.6 E-UE Provisioning Data Model

The IPCablecom provisioning data model allows for a many-to-many relationship among users, devices, and applications. For more information on the data model and any data elements referenced in this Recommendation, please refer to the IPCablecom E-UE Provisioning Data Models specification ([PKT-EUE-DATA]).

6 E-UE provisioning framework

This clause presents the normative requirements for the E-UE Provisioning Framework, based on IPCablecom Device Provisioning. It includes references to IPCablecom Device Provisioning, and any necessary enhancements to support IPCablecom E-UEs.

The framework aims to reuse all the IPCablecom Device Provisioning interfaces, and supports all three provisioning flows: Basic, Hybrid and Secure. For more information on IPCablecom Device Provisioning please refer to [PKT-PROV1.5].

Clause 6.1 presents the eUE Provisioning Interfaces. For provisioning an eCM embedded within an E-UE, please refer to [PKT-PROV1.5] and any enhancements specified in clause 6.2.1.1.

6.1 eUE Provisioning Interfaces

Figure 2 represents the network components and interfaces that form the eUE Provisioning Framework.

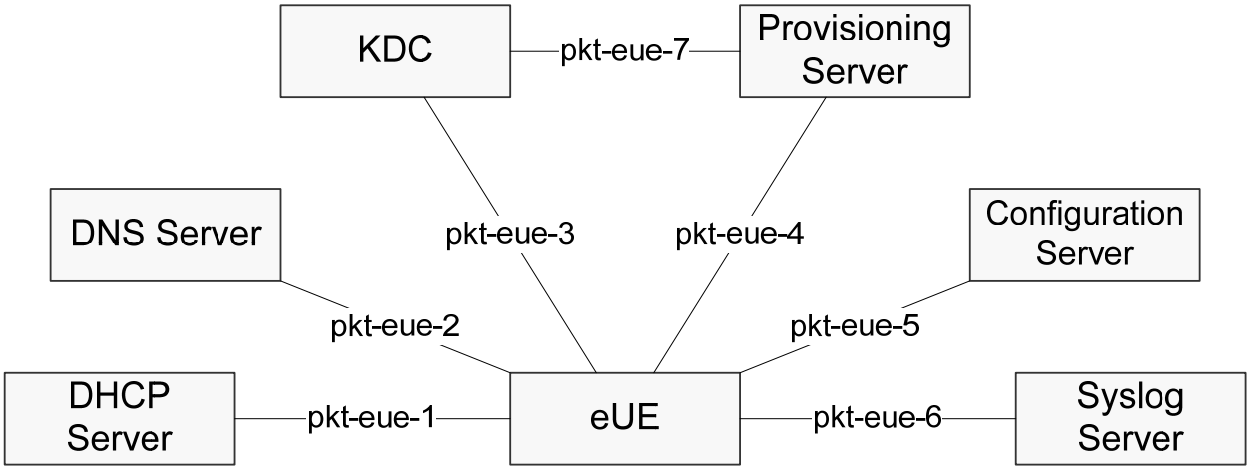

Figure 2 – E-UE Provisioning Components and Interfaces

6.1.1 pkt-eue-1

The pkt-eue-1 interface corresponds to the protocol exchanges between the eUE, acting in the role of a DHCP client, and the DHCP server. It allows the eUE to identify itself to the connecting access network, and it allows the DHCP server to provide IP configuration information such as IP addresses and DNS server addresses to the eUE. Additionally, it allows for the transport of IPCablecom-specific information, such as the choice of the provisioning flow (i.e., Basic, Hybrid or Secure).

The protocol for this interface is DHCP. The mechanism for data transport from either element (eUE or the DHCP server) that utilizes this interface is via specified DHCP options.

This interface supports two IP versions: IPv4 and IPv6. For use in IPv4 environments, eUEs and DHCP servers implementing the pkt-eue-1 interface MUST comply with the DHCP client requirements, such as DHCP protocol usage specified in this Recommendation and any additional requirements specified in [RFC2131]. For use in IPv6 environments, eUEs and DHCP servers implementing the pkt-eue-1 interface MUST adhere to the DHCP protocol usage requirements specified in this Recommendation and any additional requirements specified in [RFC3315], [RFC2461], and [RFC2462].

This interface is crucial for eUEs that are not pre-configured in an Operator's network to be identified and dynamically configured by the Operator.

6.1.2 pkt-eue-2

The pkt-eue-2 interface corresponds to the protocol exchanges between the eUE, acting in the role of a DNS client and a DNS server. It allows the UE to resolve network identifiers, such as Fully Qualified Domain Names (FQDNs), into one or more IP addresses for communication.

The eUE obtains the IP address of one or more DNS servers to communicate with as part of the IP configuration information, using pkt-eue-1. DNS servers and eUEs implementing the pkt-eue-2 interface MUST conform to the requirements in [RFC1034], [RFC1035], [RFC2782], [RFC2915], and for IPv6 use, [RFC3596].

6.1.3 pkt-eue-3

The pkt-eue-3 interface corresponds to the protocol exchanges between the eUE and the Key Distribution Center (KDC). This is based on the interface labeled pkt-p5, specified in [PKT-PROV1.5], utilizing the Kerberos requirements detailed in [PKT-SEC1.5]. It allows an Operator to mutually authenticate to a client. It also allows for the Operator to securely provide authentication and encryption keys for configuration and SNMPv3, and to enable secure configuration and secure management, respectively.

As an enhancement to support IPv6 network address, when an IPv6 address is used as a second component of the Kerberos Principal Name, the address MUST be formatted according to the ABNF notation ([RFC2234]) provided below:

```
IPv6Address = "[" 7 (h16 ":") h16 "]"
h16 = 4 LCHEXDIG
LCHEXDIG = DIGIT / "a" / "b" / "c" / "d" / "e" / "f"
DIGIT =   "0" / "1" /"2" /"3" /"4" /"5" /"6" /"7" /"8" /"9"
```

As an example, `df/[805B:2D9D:DC28:0000:0000:FC57:D4C8:1FFF]` is a valid representation.

Examples of invalid Principal Names for the IPv6 Addresses are provided below:

```
Example: df/[ FF00:4501::32]
Reason: Trailing zero-compression is used

Example: df/[0:0:0:0:0:FFFF:129.144.52.38]
Reason: Alternative form for IPv4/IPv6 environments is used.
```

```
Example: df/[805B:2D9D:DC28:0:0:FC57:D4C8:1FFF]
Reason: The least significant zeros are omitted from the hexadecimal numbers in the IPv6
address.
```

KDC servers and eUEs that implement the pkt-eue-3 interface MUST comply with the requirements specified in [PKT-PROV1.5], [PKT-SEC1.5], and for IPv6, the enhancements presented in this clause.

6.1.4 pkt-eue-4

The pkt-eue-4 interface corresponds to the interactions between the eUE and the Provisioning Server. The properties of this interface are dependent on the provisioning flow.

In the Basic Provisioning Flow it can be optionally used to report the configuration file status using SNMP. Provisioning Servers and eUEs that implement the pkt-eue-4 interface and support the Basic Provisioning Flow MUST comply with the requirements for the Basic Provisioning Flow indicated in [PKT-PROV1.5].

In the Hybrid Provisioning Flow it serves two purposes. It is used to request and obtain configuration information such as configuration file name, location, protocol, and the authentication key. It is also used to optionally report the configuration file status. The protocol used is SNMP. Provisioning Servers and eUEs that implement the pkt-eue-4 interface and support the Basic Provisioning Flow MUST comply with the requirements for the Hybrid Provisioning Flow indicated in [PKT-PROV1.5].

In the Secure Provisioning Flow, it serves two purposes. It is used to request and obtain secure configuration information such as configuration file name, location, protocol, the authentication key, and optionally, the privacy key. It is also used to report the configuration file status. The protocols used are Kerberos (for authentication prior to requesting configuration) and SNMP. Provisioning Servers and eUEs that implement the pkt-eue-4 interface and support the Secure Provisioning Flow MUST comply with the requirements for the Secure Provisioning Flow indicated in [PKT-PROV1.5] and the corresponding Kerberos requirements in [PKT-SEC1.5].

6.1.5 pkt-eue-5

The pkt-eue-5 interface corresponds to the interactions between the eUE and the Configuration Server. The configuration parameters are delivered to the eUE via a TLV (Type-Length-Value) formatted binary configuration file.

The protocols used are TFTP, or optionally, HTTP. Provisioning Servers and eUEs implementing the pkt-eue-5 interface MUST comply with the configuration file requirements using the TFTP protocol as specified in [PKT-PROV1.5]. Provisioning Servers and eUEs MAY also comply with the configuration file requirements using the HTTP protocol as specified in [PKT-PROV1.5].

6.1.6 pkt-eue-6

The pkt-eue-6 interface corresponds to the interactions between the eUE and the Syslog Server for reporting management events, as specified in [PKT-MEM1.5] and controlled via the Management Event MIB specified in [PKT-EUE-DATA]. The management events can be used for monitoring and troubleshooting the eUE and associated applications.

Syslog Servers and eUEs implementing the pkt-eue-6 interface MUST comply with the interface, messaging, and reporting requirements specified in [PKT-MEM1.5], except for enhancements such as the MIB module specified in [PKT-EUE-DATA].

The Syslog Server address is obtained via DHCP (option 7). If eUE is provided with multiple Syslog Servers via DHCP, it MUST use the first Syslog Server address for management event transmissions.

6.1.7 pkt-eue-7

The pkt-eue-7 interface corresponds to the interactions between the KDC and the Provisioning Server. It allows a KDC authenticating the eUE's certificate to ensure that the request originated from the same IP address and using the same FQDN as provided by the DHCP server using pkt-eue-1. This interface is specified in [PKT-SEC1.5]. To support IPv6 addresses, the enhancement indicated in Table 1 is proposed to the KRB_SAFE message used by this interface.

Table 1 – KRB_SAFE Data Format

Field Name	Length	Description
Message Type	1 byte	2 = eUE FQDN and IP Reply
Enterprise Number	4 bytes	Network byte order, MSB first. 1 = IPCablecom
Protocol Version	1 byte	2 for this version
eUE FQDN	variable	eUE FQDN
eUE IP address	4 bytes (for IPv4) or 16 bytes (for IPv6)	eUE-IP address (MSB first)

Provisioning Servers and KDCs implementing the pkt-eue-7 interface MUST support the mapping of the MTA MAC address to FQDN (and optionally the IP address) as specified in [PKT-SEC1.5].

6.2 E-UE Provisioning Components

This clause details the network components that utilize the interfaces specified in clause 6.1, and the associated requirements. It also summarizes the additional requirements required by this framework for the DOCSIS elements to support the framework specified by this Recommendation.

6.2.1 E-UE

The E-UE is an IPCablecom Embedded UE, and by definition, is an eDOCSIS device. Thus, the eCM and the eUE MUST conform to the eDOCSIS eCM and eSAFE requirements, respectively, as specified in the eDOCSIS specification ([eDOCSIS]).

The following E-UE requirements apply:

- The E-UE MUST support a monolithic software image, i.e., one software image that supports both eCM and eUE components.
- The E-UE MUST support the Software Download mechanism specified by corresponding DOCSIS specifications.

6.2.1.1 eCM

The eCM MUST follow the requirements specified in the DOCSIS and eDOCSIS suite of specifications, with any enhancements specified in this Recommendation.

The additional eCM requirements are as follows:

- The eCM component of an E-UE MUST support the IPCablecom-specific DHCP options as required by the provisioning flows specified in this Recommendation.
- The eCM component of an E-UE MUST relay the IPCablecom-specific DHCP options obtained during eCM provisioning to the eUE component.
- The eCM component of an E-UE MUST support, and attempt, time retrieval from a ToD server prior to eUE provisioning. This is required for the Secure Provisioning Flow. If unavailable, the eCM MUST make suitable retry attempts, similar to DHCP backoff and retry, prior to eUE initialization.

6.2.1.2 eUE

The following eUE requirements apply:

- The eUE MUST have its own MAC address, different from the MAC address of the eCM.
- The eUE MUST have its own IP address, different from the IP address(es) of the eCM.
- The eUE MUST be able to operate in environments where the eUE IP address may either be in the same, or in a different IP subnet, as the eCM.
- The eUE MUST reject DHCP offers (i.e., DHCPv6 ADVERTISE messages) with link-local IPv6 addresses when it is being provisioned in IPv6 mode.
- The eUE configuration file MUST be different from the eCM configuration file.
- The eUE MUST support all the interfaces, and associated requirements specified in clause 6.1.
- The eUE MUST support all three provisioning flows: Basic, Hybrid and Secure, as specified in this Recommendation, based on [PKT-PROV1.5].
- The eUE MUST support the configuration file format specified in this Recommendation and the data element definitions specified in [PKT-EUE-DATA].
- The eUE MUST support the management requirements specified in this Recommendation.
- The eUE MUST comply with all the eMTA non-data requirements specified in [PKT-PROV1.5] unless enhanced or modified in this Recommendation.

6.2.2 DHCP Server

The DHCP Server is responsible for IP configuration. Within the E-UE Provisioning framework, it also supports IPCablecom-specific configuration such as the choice of provisioning flow (Basic, Hybrid or Secure).

A DHCP Server implementing this specification MUST support interface pkt-eue-1 and all the DHCP options that are specified for the three provisioning flows in this Recommendation. Further, a DHCP server supporting dynamic configuration MUST provide the eUE 3-tuple consisting of an eUE mac address, eUE assigned IP address, or eUE assigned FQDN to the Provisioning Server for use with the interface pkt-eue-7. A DHCP Server SHOULD also support dynamic DNS updates to the DNS server and maintain a real time mapping of IP addresses and FQDN for each eUE that it configures.

6.2.3 DNS Server

The DNS Server is responsible for resolving DNS identifiers, such as Fully Qualified Domain Names (FQDNs), for eUE. As such, a DNS Server implementing this specification MUST support the interface pkt-eue-2 and all DNS record types, such as DNS SRV, that are used within the framework specified in this Recommendation.

6.2.4 KDC

The KDC is the authenticating entity for a network, used exclusively in the case of the Secure Provisioning Flow. It allows an eUE to mutually authenticate itself to the network and facilitates secure configuration and management.

A KDC implementing this specification MUST support interfaces pkt-eue-3 and pkt-eue-7, as specified in this Recommendation. The KDC MUST also support applicable Secure Provisioning Flow requirements, as specified in this Recommendation.

6.2.5 Provisioning Server

The Provisioning Server facilitates eUE provisioning, and acts as the authorizing entity, in Hybrid and Secure Provisioning Flows. In the Secure Provisioning Flow, it allows an eUE to present

authentication credentials (using Kerberos), establish SNMPv3, request and obtain configuration information in a secure manner. In the Hybrid Flow, it allows for an eUE to request and obtain configuration information. Additionally, in the case of the Secure Provisioning Flow, the Provisioning Server relays the 3-tuple (consisting of eUE mac address, eUE IP address, and eUE FQDN) provided during the IP configuration stage – to the KDC for authentication.

A Provisioning Server implementing this specification MUST implement interfaces pkt-eue-4 and pkt-eue-7, as specified in this Recommendation.

6.2.6 Configuration Server

The Configuration Server is a data store that provides configuration data to the eUEs. A Configuration Server implementing this specification MUST implement the interface pkt-eue-5, and any requirements associated with the provisioning flows, as specified in this Recommendation.

6.2.7 Syslog Server

The Syslog Server collects syslog messages transmitted as part of the Management Event Framework specified in [PKT-MEM1.5]. A Syslog Server MUST implement the interface pkt-eue-6 and any requirements associated with it, as specified in this Recommendation.

6.2.8 Additional Component Requirements

In addition to the requirements shown above, this specification adds additional requirements to components associated with the eCM. These are summarized in this clause.

6.2.8.1 eCM DHCP Server

In addition to the DOCSIS requirements, the eCM DHCP Server MUST support the IPCablecom-specific DHCP options as required by the provisioning flows specified in this Recommendation. The eCM's DHCP Server SHOULD provide the eCM with ToD information for other purposes, such as management events. In deployments using the Secure Provisioning Flow, the eCM DHCP Server MUST provide the eCM with the ToD Server information.

6.2.8.2 eCM Time of Day (ToD) Server

Deployments using the Secure Provisioning Flow need the ToD server to ensure successful eUE provisioning. In this framework, the eUE learns the network time by relying on the time provided to the eCM component. This is also useful to analyse events generated as part of the management event mechanism framework.

As a note, while the Secure Provisioning Flow utilizes Universal Coordinated Time (UTC), fluctuations in application times due to events such as Daylight Savings Time or Operating System patches needs to be considered by Operators.

6.3 E-UE Provisioning Flows

The E-UE contains two logical components: eCM and eUE. Thus, E-UE Provisioning involves the provisioning of both the eCM and the eUE. Now, the eCM and eUE components can independently support IPv4, IPv6 or both (dual-stack). DOCSIS specifications allow a dual-stack eCM to be provisioned in IPv4, IPv6 or both modes. However, this framework requires that a dual-stack eUE be provisioned only in IPv4 or IPv6 modes, a choice that is provided to the eCM component as part of its IP configuration.

Once the eCM is provisioned, the eUE is initialized, if instructed to do so, via the presence of usable IPCablecom-specific options in the eCM's DHCP process. If initialized, the eUE is provided with the DHCP Server information, and if it supports dual-stack, the IP mode to use for provisioning. The eUE then attempts provisioning with the provided parameters. If the eUE successfully provisions, it is provided with the configuration necessary to participate in an IPCablecom network.

The following subclauses detail these processes and associated requirements for both the eCM and the eUE.

6.3.1 eCM Provisioning

The eCM provisioning is accomplished using the procedures specified by DOCSIS and eDOCSIS, with additional enhancements to support the framework specified in this Recommendation. This clause summarizes these processes and the enhancements. A eCM implementing the framework specified in this document MUST comply with applicable DOCSIS and eDOCSIS specifications, and the enhancements identified in this clause. The procedures for eCM provisioning in IPv4 mode is indicated in Table 2. The procedures for eCM provisioning in IPv6 mode is indicated in Table 3.

A dual-stack eCM that obtains IP configuration information from multiple DHCP servers MUST use the primary DHCP server – designated to provide the eCM configuration information – for obtaining IPCablecom specific options. For more information on DOCSIS requirements, please refer to the DOCSIS suite of specifications.

Table 2 – eCM Provisioning Flow During IPv4 Address Acquisition

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
NOTE: Refer to the DOCSIS specifications for a complete description of flows CM1-CM10. Refer to the eDOCSIS specifications for eDOCSIS specific requirements. Refer to [PKT-PROV1.5] for DHCP option 122. Refer to clause 6.4.1 for DHCP options CL_V4OPTION_CCCV6 and CL_V4OPTION_IP_PREF.			
CM1	The eCM sends a broadcast DHCPv4 discover message as specified in DOCSIS and eDOCSIS. Additionally, an eCM embedded within an E-UE MUST request the following E-UE Provisioning specific DHCP options: – CCC(122) within DHCPv4 option 55 if the eUE supports IPv4 – OPTION_V-I_VENDOR_OPTS(125) containing CL_V4OPTION_CCCV6(123) if the eUE supports IPv6 If the eUE supports dual-stack operation, the eCM MUST request both the above options.	The eCM MUST attempt IPv4 configuration with CM1.	If there is a failure in CM1, the eCM MUST behave as specified in DOCSIS.

Table 2 – eCM Provisioning Flow During IPv4 Address Acquisition

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
CM2	One or more DOCSIS DHCPv4 Servers respond with DHCP OFFER messages. A DOCSIS DHCPv4 Server configured to support eUEs MUST include the requested E-UE Provisioning specific DHCPv4 options: 122, CL_V4OPTION_CCCV6, or both. If both the options are provided, the DOCSIS DHCPv4 Server MUST also include the DHCP option CL_V4OPTION_IP_PREF indicating a choice between IPv4 and IPv6 for eUE operation. A DOCSIS DHCPv4 Server that is prohibited from enabling the eUE component associated with the eCM SHOULD comply with the corresponding requirements regarding DHCP option codes 122 and CL_V4OPTION_CCCV6. This would allow for faster provisioning of the eCM by eliminating retry attempts indicated in CM3. A DOCSIS DHCPv4 Server without any knowledge of E-UE Provisioning MAY respond with DHCP OFFERs without including any of the requested DHCP options, 122 or CL_V4OPTION_CCCV6.	The eCM DHCP Server MUST respond with CM2 only after the successful completion of CM1, per DOCSIS.	If there is a failure in CM2, the eCM MUST behave as specified in DOCSIS.

Table 2 – eCM Provisioning Flow During IPv4 Address Acquisition

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
CM3	Upon receiving one or more DHCP OFFERs, the eCM MUST verify the presence of the requested E-UE Provisioning specific DHCP options 122, CL_V4OPTION_CCCV6, or both. If it requested both options: the eCM MUST be prepared to receive at least one to satisfy the criteria for requested options. the eCM MUST give precedence to a response that contains both, along with CL_V4OPTION_IP_PREF, if such a DHCP OFFER is available. As a note, the eCM MUST ignore E-UE provisioning specific option that was not requested. For example, if only 122 was requested and it obtained CL_V4OPTION_CCCv6, the latter is ignored. The eCM MUST then attempt to select amongst the DHCP OFFERs that contains the requested DHCP options. If none of the DHCP OFFERs satisfy the criteria for requested DHCP options, the eCM MUST retry the DHCP DISCOVER process (CM1) three times using an exponential retry method (e.g., 2, 4, 8 second intervals). After the retry attempt is completed, if none of the DHCP OFFERs contain the requested options, the eCM MUST select amidst one of the DHCP OFFERs. The eCM then sends a DHCP REQUEST message indicating the DHCPv4 server that provided the chosen DHCP OFFER.	The eCM MUST respond with CM3 only after CM2 occurs, as specified in DOCSIS.	If there is a failure in CM3, the eCM MUST behave as specified in DOCSIS.
CM4	The chosen DHCPv4 server receiving the DHCP REQUEST sends the eCM component a DHCP ACK message to confirm the IP configuration parameters such as the IP address. The DHCP Server MUST ensure that the DHCP ACK contains all the DHCP options and sub-options previously transmitted in CM2 (DHCP OFFER). If the option content of this DHCP ACK differs from the preceding DHCP OFFER, the eCM MUST treat the option content of the DHCP ACK as authoritative.	The eCM DHCP Server MUST respond with CM4 only after the successful completion of CM3, per DOCSIS.	If there is a failure in CM4, the eCM MUST behave as specified in DOCSIS.

Table 2 – eCM Provisioning Flow During IPv4 Address Acquisition

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
CM5-CM10	The eCM then completes the remainder of the DOCSIS specified registration sequence. This includes downloading the DOCSIS configuration file, requesting time of day registration, and registering with the CMTS.	The eCM MUST complete steps CM5-CM10, as specified in DOCSIS.	If there is a failure in steps CM5-CM10, the eCM MUST behave as specified in DOCSIS.

Table 3 – eCM Provisioning Flow During IPv6 Address Acquisition

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
NOTE: Refer to DOCSIS specifications for a complete description of the eCM Provisioning Flows. Refer to the eDOCSIS specifications for eDOCSIS specific requirements. Refer to [CL-CANN-DHCP-Reg] for DHCP options CL_OPTION_ORO and OPTION_VENDOR_OPTS. Refer to clause 6.4.1 for DHCP options CL_OPTION_CCCV6 and CL_OPTION_IP_PREF.			
CM1v6	The eCM transmits a DHCPv6 SOLICIT message as specified in DOCSIS and eDOCSIS. In addition, an eCM embedded within an E-UE MUST request the following E-UE Provisioning specific DHCPv6 options within CL_OPTION_ORO, the "CableLabs Option Request Option": CL_OPTION_CCC if the eUE supports IPv4 CL_OPTION_CCCV6 if the eUE supports IPv6 Both CL_OPTION_CCC and CL_OPTION_CCCv6, along with CL_OPTION_IP_PREF if the eUE supports dual-stack operation	The eCM MUST attempt IPv6 configuration with CM1v6.	If there is a failure in CM1v6, the eCM MUST behave as specified in DOCSIS.

Table 3 – eCM Provisioning Flow During IPv6 Address Acquisition

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
CM2v6	One or more DOCSIS DHCPv6 Servers respond with DHCP ADVERTISE messages. A DOCSIS DHCPv6 MUST include the requested E-UE Provisioning specific options: CL_OPTION_CCC, CL_OPTION_CCCv6, or both, within OPTION_VENDOR_OPTS. If both the options are provided, the DOCSIS DHCP Server MUST also include the DHCP option CL_OPTION_IP_PREF within OPTION_VENDOR_OPTS, indicating a choice between IPv4 and IPv6 for eUE operation. A DOCSIS DHCPv6 Server that is prohibited from enabling the eUE component associated with the eCM SHOULD comply with the corresponding requirements regarding DHCP option codes CL_OPTION_CCC and CL_OPTION_CCCV6. This would allow for faster provisioning of the eCM by eliminating retry attempts indicated in CM3v6. A DOCSIS DHCPv6 server without any prior knowledge of eUE devices MAY respond without any of the requested E-UE provisioning specific options – CL_OPTION_CCC, CL_OPTION_CCCV6, and CL_OPTION_IP_PREF.	The eCM DHCP Server MUST respond with CM2v6, only after the successful completion of CM1v6, per DOCSIS.	If there is a failure in CM2v6, the eCM MUST behave as specified in DOCSIS.
CM3v6	Upon receiving one or more DHCP ADVERTISE messages, the eCM MUST verify the presence of the requested E-UE Provisioning specific DHCP options, CL_OPTION_CCC, CL_OPTION_CCCV6, or both. If it requested both options: the eCM MUST be prepared to receive at least one to satisfy the criteria for requested options. the eCM MUST give precedence to a response that contains both, along with CL_OPTION_IP_PREF, if such a DHCP ADVERTISE is available. As a note, the eCM MUST ignore E-UE provisioning specific option that was not requested. For example, if only CL_OPTION_CCC was requested and it obtained CL_OPTION_CCCv6, the latter is ignored. The eCM MUST then attempt to select amongst the DHCP ADVERTISE messages that contains the requested DHCP options.	The eCM MUST respond with CM3v6, only after CM2v6 occurs, as specified in DOCSIS.	If there is a failure in CM3v6, the eCM MUST behave as specified in DOCSIS.

Table 3 – eCM Provisioning Flow During IPv6 Address Acquisition

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
	If none of the DHCP ADVERTISE messages satisfy the criteria for requested DHCP options, the eCM MUST retry the DHCP SOLICIT process (CM1v6) three times using an exponential retry method (e.g., 2, 4, 8 second intervals). After the retry attempt is completed, if none of the DHCP ADVERTISE messages contain the requested options, the eCM MUST select amidst one of the DHCP ADVERTISE messages. Once a DHCP ADVERTISE message has been selected, the eCM sends a DHCPv6 REQUEST message.		
CM4v6	The chosen DHCPv6 server receiving the DHCP REQUEST sends the eCM component a DHCP REPLY message to confirm the IP configuration parameters such as the IP address. The DHCP Server MUST ensure that the DHCP REPLY message contains all the DHCP options and sub-options previously transmitted in CM2v6 (DHCP ADVERTISE). If the option content of this DHCP REPLY differs from the preceding DHCP ADVERTISE message, the eCM MUST treat the option content of the DHCP REPLY as authoritative.	The eCM DHCP Server MUST respond with CM4v6 only after the successful completion of CM3v6, per DOCSIS.	If there is a failure in CM4v6, the eCM MUST behave as specified in DOCSIS.
CM5v6 – CM10v6	The eCM MUST complete the remainder of the DOCSIS specified registration sequence, as per DOCSIS. The E-UE then proceeds to initialize the eUE as specified in clause 6.3.4.	The eCM MUST complete steps CM5v6 – CM10v6, per DOCSIS.	If there is a failure in steps CM5v6 – CM10v6, the eCM MUST behave as specified in DOCSIS.

6.3.2 eUE initialization and DHCP Server Selection

Once the eCM has completed provisioning, the decision to initialize the eUE can be made. This is based on the requested E-UE provisioning specific DHCP options during eCM provisioning. Specifically, the eCM MUST take into consideration responses to only the requested E-UE provisioning specific DHCP options to decide on eUE initialization. For instance, if it solely requested CL_OPTION_CCC within the DHCPv6 SOLICIT message, it considers only the CL_OPTION_CCC provided in the DHCPv6 ADVERTISE message, and ignores DHCP option CL_OPTION_CCCv6 even if it is provided.

These options provide the eCM with the IP provisioning mode of the eUE and the eUE's DHCP server addresses. Specifically:

- DHCP options 122 and CL_OPTION_CCC are used to request the eUE's DHCPv4 server addresses.

- DHCP options CL_V4OPTION_CCC and CL_OPTION_CCCv6 are used to request the eUE's DHCPv6 server addresses.

Table 4 indicates how the responses to an eCM's request are to be interpreted within the framework specified in this Recommendation. An eCM contained within an E-UE MUST comply with Table 4 and make decisions regarding eUE initialization, and if so, the IP addressing mode to choose. As a note, when both DHCPv4 and DHCPv6 addresses are requested, the DHCP server can indicate a preference using the DHCP options CL_V4OPTION_IP_PREF and CL_OPTION_IP_PREF, respectively.

Table 4 – Options for the eCM to initialize the eUE

eCM Request	eCM's DHCP Server Response (DHCPv4 ACK or DHCPv6 RESPONSE)	eUE Provisioning Mode
eUE's DHCPv4 server address	Valid eUE DHCPv4 server options	IPv4, unless explicit indicator to shutdown the eUE (see clause 6.4.1)
	No valid eUE DHCPv4 server options (even after retry attempts)	eUE is not initialized
eUE's DHCPv6 server address	Valid eUE DHCPv6 server options	IPv6, unless explicit indicator to shutdown the eUE (see clause 6.4.1)
	No valid eUE DHCPv6 server options (even after retry attempts)	eUE is not initialized
eUE's DHCPv4 or DHCPv6 Server addresses	Preference for eUE DHCPv4 server option; valid DHCPv4 server options provided	IPv4, unless explicit indicator to shutdown the eUE (see clause 6.4.1)
	Preference for eUE DHCPv6 server option; valid DHCPv6 server options provided	IPv6, unless explicit indicator to shutdown the eUE (see clause 6.4.1)
	No preference provided; contained valid eUE DHCPv4 server options	IPv4, unless explicit indicator to shutdown the eUE (see clause 6.4.1)
	No preference provided; contained valid eUE DHCPv6 server options only	IPv6, unless explicit indicator to shutdown the eUE (see clause 6.4.1)
	No preference provided; contained both options	IPv6, unless explicit indicator to shutdown the eUE (see clause 6.4.1)
	Preferred options are not valid, or no options were provided (even after retry attempts)	eUE is not initialized

Based on Table 4, the eUE is either initialized or disabled. If the eUE is initialized, the eCM MUST provide the IP addressing mode and the corresponding DHCP server options. Depending on the addressing mode, the eUE proceeds to provision in IPv4 or IPv6 addressing modes. When the eUE is disabled, it MUST NOT respond to Neighbor Discovery and Router Solicitation messages. Once disabled as such, the eUE MUST remain disabled until reinitialized by the eCM.

6.3.3 eUE Provisioning in the IPv4 Addressing Mode

If the eUE is initialized in IPv4 addressing mode, it MUST implement the Power-on Initialization Flow specified in [PKT-PROV1.5], clause 7.2.1 titled "Embedded-MTA Secure Power-on Initialization Flow (IPv4 eCM)". An eUE initialized in IPv4 addressing mode MUST also comply with [RFC4361].

6.3.4 eUE Provisioning in the IPv6 Addressing Mode

If the eUE is initialized in IPv6 addressing mode, it MUST perform the following processes in the prescribed order.

- Link-local address assignment.
- Router discovery.
- IP configuration retrieval using DHCPv6.

The requirements associated with each process are specified in the following subclauses.

6.3.4.1 Link-local Address Assignment

The following requirements apply for eUE link-local address assignment:

- The eUE MUST construct a link-local address for its management interface according to the procedures specified in [RFC2462].
- The eUE MUST use the EUI-64 (64-bit Extended Unique Identifier) as a link-local address for its management interface as described in [RFC3513].
- The eUE MUST use Duplicate Address Detection (DAD), as described in [RFC2462], to confirm that the constructed link-local address is not already in use. If the eUE determines that the constructed link-local address is already in use, the eUE MUST report the event in its local log, stop the IPv6 process, not assign the tentative EUI-64 address to the interface, and wait for manual intervention.

6.3.4.2 Router Discovery

After successful link-local address assignment is accomplished, the eUE MUST perform the discovery of the default and neighboring routers, as specified in [RFC2461], by sending Router Solicitation (RS) messages. The eUE MUST identify neighboring routers and default routers from valid Router Advertisement (RA) messages obtained in response.

Valid RAs are RAs that:

- are correctly formatted as specified in [RFC2461];
- have the M bit set to 1, indicating the stateful address configuration (DHCPv6).

If an eUE does not receive any valid RAs within the specified retry attempts, the eUE MUST proceed as if provisioning in IPv6 addressing mode has failed and re-initialize the eUE with IP configuration.

6.3.4.3 IP Configuration Retrieval Using DHCPv6

Once the eUE has completed router discovery, it MUST follow the steps shown in Figure 3 – eUE Provisioning Flow in IPv6 Addressing Mode and explained in Table 5 – eUE Provisioning Flow for IPv6 Addressing. The eUE MUST NOT use DHCPv6 Rapid Commit during this flow.

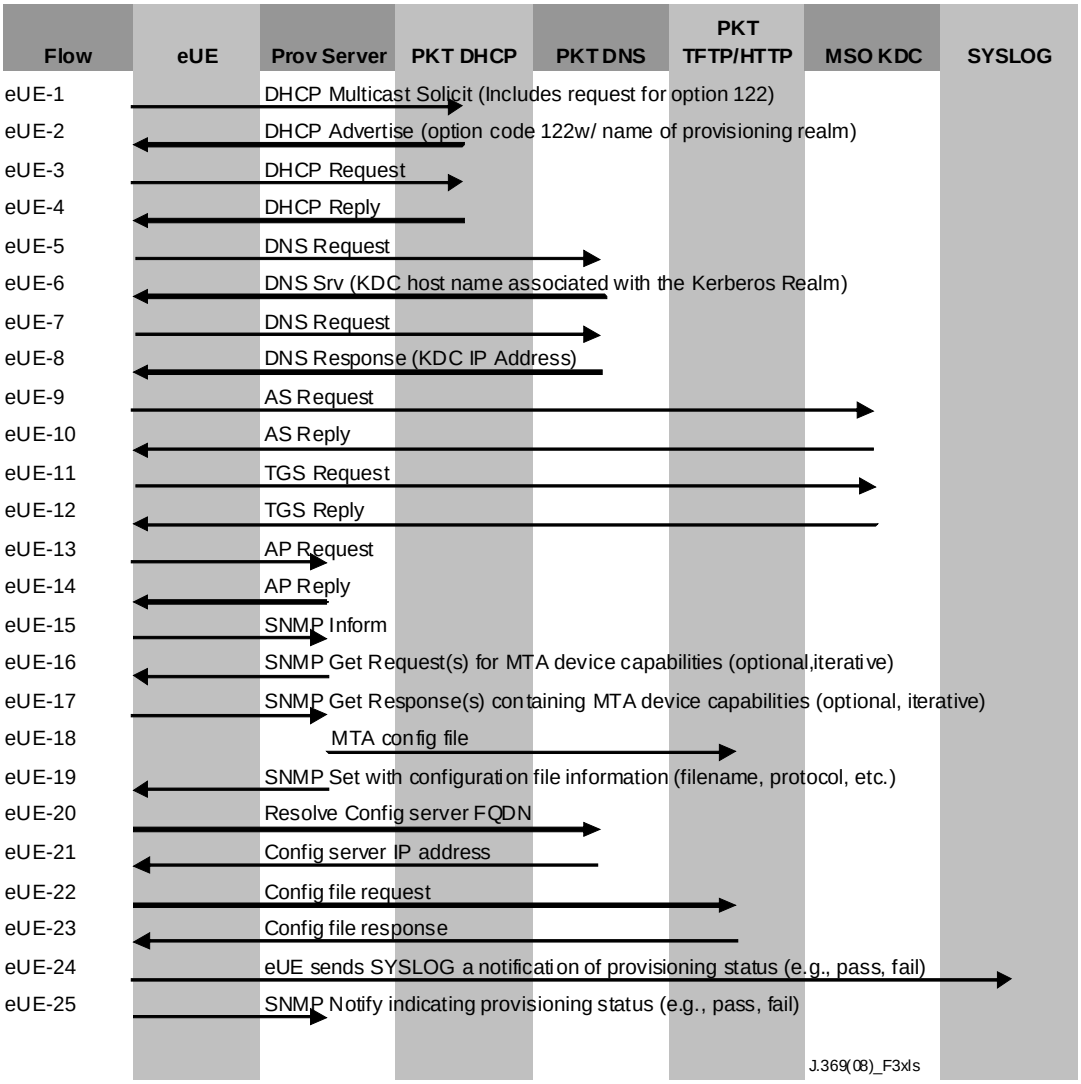

Figure 3 – eUE Provisioning Flow in IPv6 Addressing Mode

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
NOTE: Refer to [CL-CANN-DHCP-Reg] for DHCP option CL_OPTION_MODEM_CAPABILITIES. Refer to clause 6.4.1 for DHCP option CL_OPTION_CCCV6.			
eUE-1	DHCPv6 SOLICIT Message The eUE MUST send a multicast DHCPv6 SOLICIT message which includes OPTION_FQDN as specified in [RFC4704] with the following requirements: – "domain-name" field of this option is to be empty; – "flags" field of this option is set as follows: S=1, O=0, N=0.	The eUE MUST NOT proceed eUE-1 prior to successful completion of CM10v6.	If failure per DHCP protocol, the eUE MUST repeat eUE-1.

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
	The eUE MUST include the following in the DHCPv6 SOLICIT message: – Client Identifier option containing the DUID (DHCP Unique Identifier) for the eUE, as specified by [RFC3315]. The eUE can choose any one of the rules to construct the DUID according to clause 9.1 of [RFC3315]; – CL_OPTION_MODEM_CAPABILITIES, as specified in [CL-CANN-DHCP-Reg]. The eUE MUST also request the following DHCPv6 options: – OPTION_CLIENTID (1) – OPTION_IAADDR (5) – OPTION_ORO (6) – OPTION_VENDOR_OPTS (17) – CL_OPTION_TFTP_SERVERS (32) – CL_OPTION_CONFIG_FILE_NAME (33) – CL_OPTION_SYSLOG_SERVERS (34) – OPTION_DNS_SERVERS (23) – CL_OPTION_DEVICE_ID (36) – OPTION_FQDN – CL_OPTION_CCCV6		
eUE-2	DHCPv6 ADVERTISE Message An eUE DHCP Server that is configured to respond to eUE requests MUST send a DHCP ADVERTISE message in response to the DHCP SOLICIT message. An eUE DHCP Server that is configured to provision eUEs MUST include the requested DHCP options. An eUE DHCP Server that is configured to disable the eUE requesting DHCP configuration MUST include CL_OPTION_CCCV6 and explicitly prohibit provisioning as indicated in clause 6.4.1. A DHCP Server that is unaware of eUE provisioning MAY respond without the requested DHCP options.	The eUE DHCP Server MUST NOT proceed with eUE-2 before successful completion of eUE-1, per [RFC3315].	If failure per DHCP protocol, the eUE MUST restart with eUE-1.

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
eUE-3	DHCPv6 REQUEST Message After sending the DHCP SOLICIT message, the eUE MUST await valid DHCP ADVERTISE messages as specified in [RFC3315]. A valid DHCP ADVERTISE is specified as one that originates from the allowed list of eUE DHCP servers (as indicated by the eCM), and contains CL_OPTION_CCCV6 with valid sub-options 3 and 6. If it does not obtain any valid DHCP ADVERTISE messages, the eUE MUST consider this step as failed. If it obtains one or more valid DHCP ADVERTISE messages, the eUE MUST provide priority to the DHCP ADVERTISE messages in the following order, based on the value contained in sub-option 3 of CL_OPTION_CCCV6. Those without the opaque value of the ASCII string NONE Those indicating Secure Provisioning Flow, i.e., a non-reserved Kerberos Realm indicator. Those indicating Hybrid Provisioning Flow, i.e., a value of HYBRID.1 or HYBRID.2. Those indicating Basic Provisioning Flow, i.e., a value of BASIC.1 or BASIC.2. Additionally, the following requirements apply. If there is at least one DHCP ADVERTISE message with a value other than NONE in sub-option 3 of CL_OPTION_CCCV6, it MUST proceed with DHCP Server selection process. If there is at least one DHCP ADVERTISE message with a value of NONE in sub-option 3 of CL_OPTION_CCCV6, and there are no DHCP ADVERTISE messages with an alternate value, the eUE MUST NOT continue any further in the DHCP process, and disable itself until reinitialized. If the eUE received valid DHCP ADVERTISE messages that it can select from, it MUST select a DHCP Server and respond with a DHCP REQUEST message.	The eUE DHCP Server MUST NOT proceed with eUE-3 before waiting for eUE-2 to complete, as indicated by [RFC3315].	If failure per DHCP protocol, the eUE MUST restart with eUE-1.

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
eUE-4	DHCPv6 REPLY Message The DHCP Server sends a DHCPv6 REPLY message to the eUE to confirm IP configuration parameters such as CL_OPTION_CCCV6. The DHCP Server MUST ensure that the DHCP REPLY message contains all the DHCP options and sub-options previously transmitted in eUE-2 (DHCP ADVERTISE). If the option and sub-option values of the DHCP REPLY differ from the preceding DHCP ADVERTISE (eUE-2), the eUE MUST treat the DHCP REPLY message as authoritative. If the DHCPv6 REPLY Message is not valid as per the criteria established in eUE-2, the eUE MUST fail this step. The eUE MUST perform a Duplicate Address Detection ([RFC2462]) with the IPv6 address. If the eUE determines through DAD the IPv6 address assigned through the DHCPv6 server is already in use by another device, the eUE MUST send a DHCPv6 DECLINE message to the DHCPv6 server and consider this step as failed.	The eUE DHCP Server MUST NOT proceed with eUE-4 before successful completion of eUE-3, per [RFC3315].	If failure per DHCP protocol, the eUE MUST return to eUE-1.
NOTE – The provisioning flow forks into one of three directions as follows: If the eUE-4 DHCPv6 REPLY message indicates the Basic Flow, the eUE MUST use the Basic Provisioning as described in [PKT-PROV1.5], clause titled "Embedded-MTA Power-On Initialization Flow (Basic Flow)". If the eUE-4 DHCPv6 REPLY message indicates the Hybrid Flow, the eUE MUST use the Hybrid Provisioning Flow as described in [PKT-PROV1.5], clause titled "Embedded-MTA Power-On Initialization Flow (Hybrid Flow)". In either of the above cases, the steps involved would be performed in an IPv6 environment. Otherwise, the Secure Flow is indicated, and the eUE MUST proceed to step eUE-5 below.			
eUE-5	DNS SRV Request The eUE requests the MSO KDC host name for the Kerberos realm.	The eUE MUST proceed with eUE-5, if Secure Flow is chosen, after eUE-4 is completed.	If the step fails, the eUE MUST restart with eUE-1.
eUE-6	DNS SRV Reply Returns the MSO KDC host name associated with the provisioning REALM.	The DNS Server MUST perform eUE-6 after eUE-5 is completed.	If the step fails, the eUE MUST restart with eUE-1.
eUE-7	DNS Request (optional) The eUE now requests the IP Address of the MSO KDC via AAAA records.	The eUE MUST proceed with eUE-7 if eUE-6 did not provide AAAA records.	If the step fails, the eUE MUST restart with eUE-1.

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
eUE-8	DNS Reply The DNS Server returns the IP Address of the MSO KDC.	The DNS Server MUST proceed with eUE-8, after eUE-7 is completed.	If the step fails, the eUE MUST restart with eUE-1.
eUE-9	AS Request The AS Request message is sent to the MSO KDC to request a Kerberos ticket.	If the eUE does not have a valid, stored, ticket that can be used, it MUST proceed with eUE-9 after eUE-8 is completed.	If the step fails, the eUE MUST restart with eUE-1. The failure conditions are specified in [PKT-SEC1.5].
eUE-10	AS Reply The AS Reply Message is received from the MSO KDC containing the Kerberos ticket. NOTE – The KDC must map the eUE MAC address to the FQDN before sending the AS Reply.	The KDC MUST proceed with eUE-10 after eUE-9 is completed.	If the step fails, the eUE MUST restart with eUE-1. The failure conditions are specified in [PKT-SEC1.5].
NOTE 1 – Flows eUE-11 and eUE-12 below are optional in some cases. Refer to [PKT-SEC1.5] for more information. NOTE 2 – SNMPv3 entity (FQDN) MUST be resolved to an IP address anywhere during flows eUE-5 to eUE-12. NOTE 3 – If the eUE has a valid provisioning application server ticket saved in NVRAM, then it MUST skip the flows eUE-5 to eUE-12 in successive eUE resets (flows eUE-1 to eUE-25).			
eUE-11	TGS Request If eUE-obtained TGT in eUE-10, the TGS Request message is sent to the MSO KDC.	The eUE MUST proceed with eUE-11 after eUE-10 if TGS procedures are employed.	If the step fails, the eUE MUST restart with eUE-1. The failure conditions are specified in [PKT-SEC1.5].
eUE-12	TGS Reply The TGS Reply message is received from the MSO KDC.	The TGS MUST respond with eUE-12 after eUE-11 is completed.	If the step fails, the eUE MUST restart with eUE-1. The failure conditions are specified in [PKT-SEC1.5].

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
eUE-13	AP Request The AP Request message is sent to the Provisioning Server to request the keying information for SNMPv3.	The eUE MUST proceed with eUE-13 after: eUE-12 if TGS is employed; eUE-10 if a ticket was requested, without TGS; eUE-8 if a valid ticket exists.	If the step fails, the eUE MUST restart with eUE-1. The failure conditions are specified in [PKT-SEC1.5].
eUE-14	AP Reply The AP Reply message is received from the Provisioning Server containing the keying information for SNMPv3. NOTE – The SNMPv3 keys must be established before the next step using the information in the AP Reply.	The Provisioning Server MUST respond with eUE-14 after eUE-13 is completed.	If the step fails, the eUE MUST restart with eUE-1. The failure conditions are specified in [PKT-SEC1.5].
eUE-15	SNMP Enrollment INFORM The eUE MUST send a SNMPv3 Enrollment INFORM to the PROV_SNMP_ENTITY (specified in the sub-option 3 of the DHCPv6 CL_OPTION_CCCV6 Option). The SNMP INFORM MUST contain a "pktcMtaDevProvisioningEnrollment" object as defined in [PKT-EUE-DATA]. The PROV_SNMP_ENTITY notifies the Provisioning Application that the eUE has entered the management domain. The Provisioning Server MUST respond to a valid SNMP INFORM, per SNMP protocol.	The eUE MUST proceed with eUE-15 after eUE-14 is completed.	If the step fails per the SNMP protocol, the eUE MUST restart with eUE-1.
NOTE – The provisioning server can reset the eUE at this point in the flows. The eUE is part of the security domain and MUST respond to management requests.			

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
eUE-16	SNMPv3 GET Request (Optional) If any additional eUE device capabilities are needed by the PROV_APP, the PROV_APP requests these from the eUE via SNMPv3 Get Requests. This is done by having the PROV_APP send the PROV_SNMP_ENTITY a "get request." Iterative: The PROV_SNMP_ENTITY sends the eUE one or more SNMPv3 GET requests to obtain any needed eUE capability information. The Provisioning Application may use an SNMPv3 GET Bulk request to obtain several pieces of information in a single message.	eUE-16 is optional, the Provisioning Server MAY employ this step after eUE-15 is completed.	N/A
eUE-17	SNMPv3 GET Response Iterative: eUE sends the PROV_SNMP_ENTITY a response for each SNMPv3 GET Request. After all the Gets, or the SNMPv3 GET Bulk, finish, the PROV_SNMP_ENTITY sends the requested data to the PROV_APP.	The eUE MUST respond with eUE-17 if eUE-16 is successfully completed.	N/A
eUE-18	This Protocol is not defined by IPCablecom. The PROV_APP MAY use the information from eUE-16 and eUE-17 to determine the contents of the eUE Configuration Data file. Mechanisms for sending, storing and, possibly, creating the configuration file are outlined in eUE-19.	The Provisioning Server SHOULD proceed with eUE-18 after: eUE-17 if eUE-16 is performed; eUE-15 otherwise.	N/A
eUE-19	SNMPv3 SET The PROV_APP MAY create the configuration file at this point, or send a predefined one. A hash MUST be run on the contents of the configuration file. The configuration file MAY be encrypted. The hash and the encryption key (if the configuration file is encrypted) MUST be sent to the eUE. The PROV_APP MUST store the configuration file on the appropriate TFTP or HTTP server. The PROV_APP then instructs the PROV_SNMP_ENTITY to send an SNMP SET message to the eUE containing the following varbindings defined in [PKT-EUE-DATA]: – pktcMtaDevConfigFile – pktcMtaDevProvConfigHash – pktcMtaDevProvConfigKey.	The Provisioning Server MUST perform eUE-19 after the successful completion of: eUE-17 if dynamic queries are used, but no dynamic config file generation is employed; eUE-18 if dynamic creation of config files is employed; eUE-15 in all other cases.	If the step fails per the SNMP protocol, the eUE MUST restart with eUE-1.

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
	The Provisioning Server MUST NOT include the last MIB Object to the SNMPv3 varbinding if the eUE Configuration File is not encrypted. NOTE 1 – In the case of file download using the HTTP access method, the filename MUST be URL-encoded with a URL format compliant with [RFC2616] with exception stated in Note 3. NOTE 2 – In the case of file download using the TFTP access method, the filename MUST be URL-encoded with a URL format compliant with [RFC3617] with the exception stated in Note 3. NOTE 3 – The eUE MUST accept IPv6 addresses in colon separated format (as per [RFC4291]) embedded in URL with or without square brackets. The eUE MUST respond to a valid SNMP SET operation, per SNMP protocol.		
eUE-20	DNS Request If the URL-encoded access method contains a FQDN instead of an IPv6 address, the eUE MUST use the service provider network's DNS server (via AAAA record) to resolve the FQDN into an IPv6 address of either the TFTP Server or the HTTP Server.	The eUE MUST perform eUE-20 if the successful completion of eUE-19 resulted in an FQDN for the Configuration Server.	If the step fails per the DNS protocol, the eUE MUST restart with eUE-1.
eUE-21	DNS Reply DNS Response: DNS server returns the IP address against eUE-20 DNS request.	The DNS Server MUST perform eUE-21 in response to successful completion of eUE-20.	If the step fails per the DNS protocol, the eUE MUST restart with eUE-1.
eUE-22	TFTP/HTTP Configuration file Request To download its configuration file, the eUE MUST perform either the TFTP or HTTP protocol exchange as indicated by URL provided to the eUE in step eUE-19. For the specific details of each protocol, see [RFC1350] – for TFTP and [RFC2616] – for HTTP respectively.	The eUE MUST perform eUE-22 after: eUE-19 if DNS resolution is not required; eUE-21 if DNS resolution is required.	If the step fails per the DNS protocol, the eUE MUST restart with eUE-1.

Table 5 – eUE Provisioning Flow for IPv6 Addressing

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
eUE-23	TFTP/HTTP Configuration file Response The TFTP/HTTP Server MUST send the requested configuration file to the eUE. For the specific details of each protocol, see [RFC1350] – for TFTP and [RFC2616] – for HTTP respectively. The hash of the downloaded configuration file is calculated by the eUE and is compared to the value received in step eUE-19. If the hash values do not match, the eUE MUST fail this step. If encrypted, the configuration file MUST be decrypted. The details of the encryption/decryption and hash calculation are provided in [PKT-SEC1.5]. Refer to clause 6.4 for eUE details on the configuration file contents.	The Configuration Server MUST perform eUE-23 in response to the successful completion of eUE-22.	If the step fails per the TFTP or HTTP protocols, the eUE MUST restart with eUE-1. If the step fails due to a configuration file error, the eUE MUST proceed to eUE-24 or eUE-25 and send and indicate the error.
eUE-24	SYSLOG Notification If a Syslog Server is configured and enabled as part of the Provisioning Process (refer to step eUE-2/eUE-4 for DHCP Options and for configuration using the MEM-MIB), then the eUE MUST send the service provider's SYSLOG a "provisioning complete" event indicating the status of the provisioning operation. This notification will include the pass-fail result of the provisioning operation.	The eUE MUST perform eUE-24 after eUE-23 is completed, if SYSLOG is configured.	If a failure is detected, the eUE MAY retry this step before proceeding to eUE-25.
eUE-25	SNMP INFORM The eUE MUST send the PROV_SNMP_ENTITY (specified in DHCP CL_OPTION_CCC(122) sub-option 3) an SNMP INFORM containing a "provisioning complete" notification. The receipt of the inform is acknowledged by the response message as defined in [RFC3414]. The SNMP INFORM MUST contain the "pktcEUEDevProvisioningStatus" MIB object. NOTE – At this stage, the eUE device provisioning data is sufficient to provide any minimal services as determined by the service provider (e.g., 611). Depending on the TLV38 configuration, there might be multiple SNMP INFORMs sent to the configured SNMP Management stations. The Provisioning Server MUST respond to a valid SNMP INFORM, per SNMP protocol.	The eUE MUST perform eUE-25 after eUE-24 is completed, if SYSLOG is used; else after eUE-23 is completed.	If failure per SNMP, the provisioning process is stopped; manual interaction required unless the eUE is re-initialized by the eCM.

6.3.5 Post-Initialization Incremental Provisioning

The eUE MUST support post-initialization incremental provisioning, such as activation and de-activation of the applications and features using SNMP and the provided data elements.

IPCablecom application specifications may specify requirements specific to applications and features by extending the data model and providing any additional incremental provisioning requirements.

6.4 E-UE Configuration

6.4.1 IP Configuration

IP configuration for the eCM and eUE components are provided via the processes described in clause 6.3, using DHCP. To facilitate this, certain E-UE Provisioning specific DHCP options were utilized that are summarized in the following subclauses. These are mostly carried via vendor-specific DHCP options such as OPTION_V-I_VENDOR_OPTS(125) for DHCPv4 and OPTION_VENDOR_OPTS(17) for DHCPv6, as specified in [RFC3925] and [RFC3315], respectively.

6.4.1.1 DHCP Option 122

The CableLabs Client Configuration DHCP Option for IPv4 addressing is used by an eCM configured in IPv4 mode to collect information about the eUE's DHCPv4 Server addresses. It is specified in [RFC3495], and the usage explained in [PKT-PROV1.5]. Values for shutting down the eUE component are specified in [PKT-PROV1.5].

6.4.1.2 DHCP Option CL_V4OPTION_CCCV6

The CableLabs-specific DHCP Option is used by an eCM configured in IPv4 mode to collect information about the eUE's DHCPv6 Server addresses. It is specified in [CL-CANN-DHCP-Reg]. It is to be noted that a DHCP Server MUST restrict the length of the DHCPv6 Server Selector ID (DSS_ID) to 32 bytes. A eUE that obtains a DSS_ID that is longer MUST only consider the first 32 bytes.

6.4.1.3 DHCP Option CL_OPTION_CCC

This CableLabs-specified DHCP Option is used by an eCM configured in IPv6 mode to collect information about the eUE's DHCPv4 Server addresses. It is specified in [CL-CANN-DHCP-Reg].

6.4.1.4 DHCP Option CL_OPTION_CCCV6

This CableLabs-specific DHCP option is used by IPCablecom compliant devices to obtain IPCablecom-specific configuration during the IP address acquisition phase. It is specified in [CL-CANN-DHCP-Reg]. It is to be noted that a DHCP Server MUST restrict the length of the DHCPv6 Server Selector ID (DSS_ID) to 32 bytes. A eUE that obtains a DSS_ID that is longer MUST only consider the first 32 bytes.

6.4.1.5 DHCP Option CL_V4OPTION_IP_PREF

When a eUE supports dual stack operation and the eCM operating in IPv4 mode requests both – eUE DHCPv4 server option and eUE DHCPv6 server option – the eCM's DHCP server can use the DHCP Option CL_V4OPTION_IP_PREF to indicate a preference. This DHCP option is specified in [CL-CANN-DHCP-Reg].

6.4.1.6 DHCP Option CL_OPTION_IP_PREF

When a eUE supports dual stack operation and the eCM operating in IPv6 mode requests both – eUE DHCPv4 server option and eUE DHCPv6 server option – the eCM's DHCP server can use the

DHCP Option CL_OPTION_IP_PREF to indicate a preference. This DHCP option is specified in [CL-CANN-DHCP-Reg].

6.4.2 Device, User and Application Configuration

The eCM component of the E-UE obtains the configuration parameters for participation in a DOCSIS network via a DOCSIS configuration file. For more information, please refer to the DOCSIS specifications.

IPCablecom configuration data required for the eUE to communicate with an IPCablecom network such as device-level, user-level and application-level data is provided via the eUE configuration file. This clause defines the format and contents of the eUE configuration file. This file contains sequence of "type, length, value" (TLV) triplets that describe an eUE attribute. The 'type' part of each triple uniquely identifies the particular data item being provisioned via the Configuration File. Table 6 contains the TLV Types used for IPCablecom eUE Configuration File and requirements on using them.

Table 6 – TLV Types Used in the eUE Configuration File

TLV Type is used for	Type	Length	Value	TLV Type Description
SNMP MIB Object	11	1 byte	variable binding	The eUE and the Provisioning Server MUST follow the requirements specified in [PKT-PROV1.5] for TLV Type 11.
Vendor Specific	43	1 byte		The eUE and the Provisioning Server MUST follow the requirements specified in [PKT-PROV1.5] for TLV Type 43.
SNMP MIB Object	64	2 bytes	variable binding	The eUE and the Provisioning Server MUST follow the requirements specified in [PKT-PROV1.5] for TLV Type 64. NOTE – The use of TLV type 11 rather than TLV type 64 is recommended wherever possible.
Notification Receiver	38	1 byte	Composite (Contains sub TLVs)	The eUE and the Provisioning Server MUST follow the requirements specified in clause 6.5.
eUE Start of File	254	1 byte	0x01	The eUE and the Provisioning Server MUST follow the requirements specified in [PKT-PROV1.5] for TLV Type 254.
eUE End of File	254	1 byte	0xFF	The eUE and the Provisioning Server MUST follow the requirements specified in [PKT-PROV1.5] for TLV Type 254.

The eUE and Provisioning Server MUST implement all TLV types described in Table 6. The eUE and Provisioning Server MUST also follow the applicable requirements described in [PKT-PROV1.5], clause 9.1 titled "MTA Configuration File", for processing the configuration file data.

6.4.2.1 Device Level Configuration Data

The eUE MUST follow the requirements described in [PKT-PROV1.5], clause 9.1.1 titled "Device Level Configuration Data", with the following clarifications:

- the "Telephony Config File Start" attribute will be interpreted as the "eUE Start of File" attribute (as in Table 6);

- the "Telephony Config File End" attribute will be interpreted as the "eUE End of File" attribute (as in Table 6);
- the applicable eUE MIBs are specified in [PKT-EUE-DATA].

6.5 E-UE Management

The eCM component of an E-UE is managed via the requirements specified in the DOCSIS and eDOCSIS specifications. No additional requirements are specified in this Recommendation.

The eUE component of an E-UE is managed via SNMP. The eUE MUST implement the SNMP-related requirements as described in [PKT-EUE-DATA].

The eUE component MUST also support the Management Event Mechanism (MEM) protocol and reporting requirements specified in the Management Event Framework Specification ([PKT-MEM1.5]), with the specific data model and event requirements specified in the E-UE Provisioning Data Models Specification ([PKT-EUE-DATA]).

The eUE can establish SNMP connectivity with the Provisioning Server during the provisioning flow. Further, additional management stations can be configured via TLV38 entries specified in [PKT-PROV1.5]. In addition, to accommodate the IPv6 address space for SNMP notifications targets, the eUE MUST implement an additional sub-option for TLV38 as defined below.

Type	Length	Value
38.8	16	16 bytes of an IPv6 address in network byte order

This new sub-type is the IPv6 equivalent of 38.1 in IPv4 addressing mode. Thus, an eUE MUST comply with the requirements specified in [PKT-PROV1.5], clause 11 titled "TLV-38 SNMP notification receiver specification", with the following clarifications.

- If the eUE is in IPv4 addressing mode, it MUST ignore sub-type 38.8.
- If the eUE is in IPv6 addressing mode, it MUST consider sub-type 38.8 in lieu of 38.1, and ignore 38.1.

6.6 E-UE Additional features

6.6.1 Reporting eUE Capabilities

During E-UE provisioning, the configuration data supplied to the eUE by the Provisioning Server may depend on the particular capabilities of the eUE. For example, support for dynamic provisioning of an E-UE that is not preconfigured in the network operator's OSS. To facilitate this behaviour, the framework specified in this Recommendation allows for eUE Capabilities to be reported via DHCP. The identified capabilities are specified in Annex A. The DHCP mechanism is specified in [PKT-PROV1.5].

- An eUE supporting this framework MUST support the capability reporting requirements described in [PKT-PROV1.5], clause 10 titled "MTA device capabilities", with the following clarifications.
- An eUE provisioning in IPv4 addressing mode will use DHCPv4 option-60 as described in [PKT-PROV1.5], with the string "pktc2.0:xxxxxx" instead of "pktc1.5:xxxxxx".
- An eUE provisioning in IPv6 addressing mode acquiring an IPv6 address will use the CL_OPTION_MODEM_CAPABILITIES DHCPv6 Option specified in [CL-CANN-DHCP-Reg].
- The capabilities to be reported are specified in Annex A.
- IPCablecom applications may extend this capability to report additional data.

6.6.2 Obtaining P-CSCF Information

The E-UE MUST obtain P-CSCF information as described in [PKT-24.229], specifically Option-II using the configuration file. The E-UE MUST NOT use method-I described in [PKT-24.229].

6.6.3 eDOCSIS Impact Analysis Reporting

As specified in [eDOCSIS], the eCM has the ability to report 'Service Interruption Impact' for each eSAFE device, if in fact the data service was interrupted at the time of the query. It is to be noted that the eUE is typically associated with multiple applications (such as voice or video) and multiple instances of each service (on each configured endpoint/user). Hence, the eUE MUST report the highest possible impact across services.

IPCablecom applications are required to specify the impact level for each application.

6.6.4 Battery Backup

E-UEs supporting Battery Backup MUST support the requirements specified in the Battery Backup MIB Specification [CL-BB-MIB]. Additionally, E-UEs MUST use the identifier "EUE" when required within the context of Battery Backup (e.g., reporting values within the MIB Object upsIdentAttachedDevices).

6.6.5 Certificate Bootstrapping

E-UEs need to be configured with IMS credentials to register and communicate with an IPCablecom network. Secure configuration of such credentials can be accomplished via the Secure Provisioning Flow. For deployments using Basic and Hybrid flows, an alternative mechanism termed 'Certificate Bootstrapping' is provided.

An eUE SHOULD support Certificate Bootstrapping. The following general requirements apply.

- The eUE MUST NOT use Certificate Bootstrapping unless triggered via a management interface.
- The eUE MUST store any retrieved credentials in non-volatile storage.

For more information on the management MIB Object to initiate the process, please refer to [PKT-EUE-DATA]. When triggered via a management session, the eUE MUST establish a TLS session with the Certificate Bootstrapping Server. The following requirements apply for the TLS session:

- The eUE and the Certificate Bootstrapping Server MUST support the CipherSuite TLS_RSA_WITH_3DES_EDE_CBC_SHA as described in [RFC2246] and TLS_RSA_WITH_AES_128_CBC_SHA as described in [RFC3268].
- The eUE and the Certificate Bootstrapping Server MUST NOT use CipherSuites with NULL encryption.
- The eUE and the Certificate Bootstrapping Server MUST NOT use CipherSuites with NULL integrity or HASH protection.
- The eUE MUST authenticate the Certificate Bootstrapping Server as specified in [RFC2246], by validating a presented server certificate.
- The Certificate Bootstrapping Server MUST authenticate by the eUE as specified in [RFC2246], by validating a presented client certificate.

Once established, the eUE MUST retrieve the device profile using HTTP. The eUE credentials and user credentials contained in the retrieved document MUST be used for any subsequent authentication procedures.

IPCablecom applications planning use of this procedure MUST specify the certificate requirements on the eUE and the Certificate Bootstrapping Server.

Annex A

eUE Capabilities

(This annex forms an integral part of this Recommendation)

A.1 eUE Capabilities

An eUE MUST report all the capabilities specified in [PKT-PROV1.5], clause 10 titled "MTA device capabilities", with the following exceptions, and any enhancements provided in this clause:

- TLV 10.2 – Number of Telephony Endpoints
- TLV 10.6 – NCS Service Flow Support
- TLV 10.7 – Primary Line Support
- TLV 10.11 – Supported CODECs
- TLV 10.12 – Silence Suppression Support
- TLV 10.13 – Echo Cancellation Support
- TLV 10.16 – MTA's "IfIndex" starting number in the "IfTable"
- TLV 10.19 – T38 Version Support
- TLV 10.20 – T38 Error Correction Support
- TLV 10.21 – RFC2833 DTMF Support
- TLV 10.22 – Voice Metrics Support
- TLV 10.23 – Device MIB Support
- TLV 10.34 – MGPI Support
- TLV 10.25 – V.152 Support

It is to be noted that some of the above capabilities may be reused by IPCablecom Application Specifications.

A.2 Capability Enhancements

This TLV of subtype 5.1 (IPCablecom Version) MUST be supplied in the Capabilities String. A new value '2' is specified to indicate IPCablecom 2.0.

Type	Length	Values	Comment	Default Value
5.1	1	0	IPCablecom 1.0	None
		1	IPCablecom 1.5	
		2	IPCablecom 2.0	

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Available
Series C	Available
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 W	Available
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, 2009