PacketCable™ 2.0

E-UE Provisioning Framework Specification

PKT-SP-EUE-PROV-I07-110825

ISSUED

Notice

This PacketCable specification is the result of a cooperative effort undertaken at the direction of Cable Television Laboratories, Inc. for the benefit of the cable industry and its customers. This document may contain references to other documents not owned or controlled by CableLabs®. Use and understanding of this document may require access to such other documents. Designing, manufacturing, distributing, using, selling, or servicing products, or providing services, based on this document may require intellectual property licenses from third parties for technology referenced in this document.

Neither CableLabs nor any member company is responsible to any party for any liability of any nature whatsoever resulting from or arising out of use or reliance upon this document, or any document referenced herein. This document is furnished on an "AS IS" basis and neither CableLabs nor its members provides any representation or warranty, express or implied, regarding the accuracy, completeness, noninfringement, or fitness for a particular purpose of this document, or any document referenced herein.

Document Status Sheet

Document Control Number	PKT-SP-EUE-PROV-I07-110825
Document Title	E-UE Provisioning Framework Specification
Revision History	I01 - Released 06/11/07 I02 - Released 07/10/08 I03 - Released 05/28/09 I04 - Released 01/20/10 I05 - Released 05/27/10 I06 - Released 01/27/11 I07 – Released 08/25/11
Date	August 25, 2011
Status	~~Work in Progress~~ ~~Draft~~ **Issued** ~~Closed~~
Distribution Restrictions	~~Author Only~~ ~~CL/Member~~ ~~CL/ Member/ Vendor~~ **Public**

Key to Document Status Codes

Work in Progress   An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.

Draft   A document in specification format considered largely complete, but lacking review by Members and vendors. Drafts are susceptible to substantial change during the review process.

Issued   A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.

Closed   A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Trademarks

Contents

Figures

Tables

1 SCOPE

1.1 Introduction and Purpose

This specification describes the provisioning mechanism for PacketCable 2.0 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 document.

1.2 Document Overview

The document is structured as follows:

- Section 2 – References.

- Section 3 – Terms and Definitions.

- Section 4 – Abbreviations.

- Section 5 – Informative section providing a description of the provisioning reference architecture, components and requirements to the IP interfaces.

- Section 6 – Normative section describing the provisioning framework requirements.

- Annex A – Normative section describing the eUE device capabilities.

1.3 Requirements

Throughout this document, 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 specification.

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

"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.

2   REFERENCES

2.1   Normative References

In order to claim compliance with this specification, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this specification. Notwithstanding, intellectual property rights may be required to use or implement such normative references.

[CANN-DHCP-Reg]	CableLabs DHCP Options Registry Specification, CL-SP-CANN-DHCP-Reg-I07-110623, June 23, 2011, Cable Television Laboratories, Inc.
[CL-BB-MIB]	CableLabs Battery Backup MIB Specification, CL-SP-MIB-BB-I04-100608, June 8, 2010, Cable Television Laboratories, Inc.
[DOCSIS-MULPI]	DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification, CM-SP-MULPIv3.0-I16-110623, June 23, 2011, Cable Television Laboratories, Inc.
[eDOCSIS]	eDOCSIS Specification, CM-SP-eDOCSIS-I22-110623, June 23, 2011, Cable Television Laboratories, Inc.
[PKT-EUE-DATA]	PacketCable E-UE Provisioning Data Models Specification, PKT-SP-EUE-DATA-I07-110825, August 25, 2011, Cable Television Laboratories, Inc.
[PKT-MEM1.5]	PacketCable 1.5 Management Event Mechanism Specification, PKT-SP-MEM1.5-I05-00527, May 27, 2010, Cable Television Laboratories, Inc.
[PKT-PROV1.5]	PacketCable 1.5 Specification, MTA Device Provisioning, PKT-SP-PROV1.5-I04-090624, June 24, 2009, Cable Television Laboratories, Inc.
[PKT-SEC1.5]	PacketCable 1.5 Security Specification, PKT-SP-SEC1.5-I03-090624, June 24, 2009, Cable Television Laboratories, Inc.
[RFC 1034]	IETF RFC1034/STD0013, Domain names - concepts and facilities, November 1987.
[RFC 1035]	IETF 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 2348]	IETF RFC 2348, TFTP Blocksize Option, May 1998.
[RFC 2579]	IETF RFC 2579/STD0058, Textual Conventions for SMIv2, April 1999.
[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]	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 3986]	IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, January 2005.
[RFC 4291]	IETF RFC 4291, IP Version 6 Addressing Architecture, February 2006.
[RFC 4293]	IETF RFC 4293, Management Information Base for the Internet Protocol, April 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.
[RFC 4861]	IETF RFC 4861, Neighbor Discovery for IP Version 6 (IPv6), September 2007.
[RFC 4862]	IETF RFC 4862, IPv6 Stateless Address Auto configuration, September 2007.

2.2 Informative References

This specification uses the following informative references.

[DOCSIS-RFI]	DOCSIS Radio Frequency Interface Specification, CM-SP-RFIv1.1-C01-050907, September 7, 2005, Cable Television Laboratories, Inc.
[PKT-24.229]	PacketCable SIP and SDP Stage 3 Specification 3GPP TS 24.229, PKT-SP-24.229-I07-11825, August 25, 2011, Cable Television Laboratories, Inc.
[PKT-ARCH-TR]	PacketCable Architecture Framework Technical Report, PKT-TR-ARCH-FRM-V06-090528, May 28, 2009, Cable Television Laboratories, Inc.
[PKT-TR-DS-IP6]	PacketCable Dual Stack IPv6 Technical Report, PKT-SP-IP6-V01-110825, August 25, 2011, Cable Television Laboratories, Inc.
[RFC 3319]	IETF RFC 3319, 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, 48377 Fremont Blvd., Suite 117, Fremont, California 94538, USA, Phone: +1-510-492-4080, Fax: +1-510-492-4001, http://www.ietf.org/.

3   TERMS AND DEFINITIONS

This specification uses the following terms:

COding-DECoding	Algorithms used to compress/decompress the data representing the Voice (or Video) media traffic.
Configuration	Configuration is the process of defining and propagating data to network elements for providing services.
Data Model	An abstract model that describes representation of data in a system.
Dual-Stack Mode	The configuration of the eUE, such that both IPv4 and IPv6 addresses are acquired and used in eUE operations.
Dual-Stack Provisioning Mode	The variation of the eUE Provisioning Process, which results in activation of the Dual-Stack Mode for eUE operations. The Provisioning Flows, however, are always using only one IP address.
Dual-Stack Support	The eUE implementation feature, which indicates the presence of the support for both IP stacks – IPv4 and IPv6.
eCM	The logical DOCSIS CM component of an E-UE, complies with DOCSIS, eDOCSIS and PacketCable requirements.
eUE	The logical PacketCable UE component of an E-UE, complies with eSAFE and PacketCable requirements.
E-UE	Embedded User Equipment. A single physical device embedded with an eDOCSIS-compliant DOCSIS Cable Modem and a PacketCable eUE.
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).
Key Distribution Center	The Authentication Server which implements the Kerberos PKINIT Authentication Protocol.
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.
Single-Stack Mode	The configuration of the eUE, such that only one IP stack is activated used in eUE operations.
Single-Stack Provisioning Mode	The variation of the eUE Provisioning Process, which results in activation of the Single-Stack Mode for eUE operations.
System Logging Protocol	A protocol which defines the transport mechanism for the messages carrying various logging information.
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.

4 ABBREVIATIONS AND ACRONYMS

This specification uses the following abbreviations:

CODEC	COding-DECoding
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DPM	Dual-Stack Provisioning Mode
DSM	Dual-Stack Mode
DSS	Dual-Stack Support
DSS_ID	DHCP Server Selector ID
HTTP	Hyper Text Transfer Protocol
KDC	Key Distribution Center
MIB	Management Information Base
MSO	Multiple System Operator
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SPM	Single-Stack Provisioning Mode
SSM	Single-Stack Mode
SYSLOG	System Logging Protocol
TFTP	Trivial File Transfer Protocol
TGT	Ticket Granting Ticket
ToD	Time of the Day
UE	User Equipment

5   TECHNICAL OVERVIEW

PacketCable 2.0 is a CableLabs specification effort designed to support the convergence of voice, video, data, and mobility technologies. For more information about PacketCable 2.0, please refer to the PacketCable 2.0 Architecture Framework Technical Report [PKT-ARCH-TR]. This document is part of the PacketCable 2.0 set of specifications and technical reports that defines the base architecture and specifies the network components and protocol requirements to configure and manage E-UEs and associated users and applications in a PacketCable environment. As a note, all references to PacketCable within this document are assumed to be PacketCable 2.0 unless stated otherwise.

The framework specified for configuration and management in this document reuses the protocols and interfaces specified for Embedded Multimedia Terminal Adaptors (E-MTAs) in the PacketCable 1.5 Device Provisioning specification [PKT-PROV1.5]. As such, this document presents a specific profile of the PacketCable 1.5 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 PacketCable architecture based on SIP and the IMS, and support IPv6. The following sub-sections provide more details on E-UEs, the reuse of 1.5 Device Provisioning, and related aspects.

5.1   Embedded User Equipment (E-UE)

PacketCable 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, PacketCable clients are termed User Equipment (UE). For more information about UEs in PacketCable, please refer to the PacketCable Architecture Framework Technical Report [PKT-ARCH-TR] and the PacketCable Dual-Stack IPv6 Architecture Technical Report [PKT-TR-DS-IP6].

This document 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 PacketCable 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 document 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 specification, 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   Re-use of PacketCable 1.5 Device Provisioning

PacketCable 1.5 Device Provisioning is a configuration and management solution designed for embedded PacketCable devices, specifically the PacketCable 1.5 Embedded Multimedia Terminal Adaptors (E-MTAs). It is

based on IETF standards and protocols such as SNMP [RFC 3411], DHCP [RFC 2131], and TFTP. This is currently being used by MSOs for PacketCable 1.5 deployments.

To re-use the existing OSS infrastructure and to expedite roll out of E-UEs with minimal OSS changes, this specification offers a framework that re-uses the protocols and interfaces specified by PacketCable 1.5 Device Provisioning with enhancements to support PacketCable E-UEs. The enhancements include:

- Support for eUEs capable of Single-Stack Mode (IPv6 in addition to IPv4). This enhancement applies to versions I01 through I06 of this specification.

- Support for eUEs capable of Dual-Stack Mode (IPv4 and IPv6 concurrently active).

- Support for Dual-Stack Provisioning Mode.

- Support for eUEs connecting to a PacketCable network.

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

- All requirements regarding Telephony Services are not applicable and will be ignored.

- Any PacketCable 1.5 Signaling 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 sections.

- 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 document.

- For any conflict in requirements, this specification 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, PacketCable supports E-UEs that can be IPv4, IPv6, or both. This document 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 PacketCable 1.5 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 MSO.

The eCM component of an E-UE is governed by the DOCSIS specifications and any enhancements provided explicitly in this document, such as PacketCable-specific DHCP options. The provisioning of the eUE is accomplished using the provisioning flows specified in this document. 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.
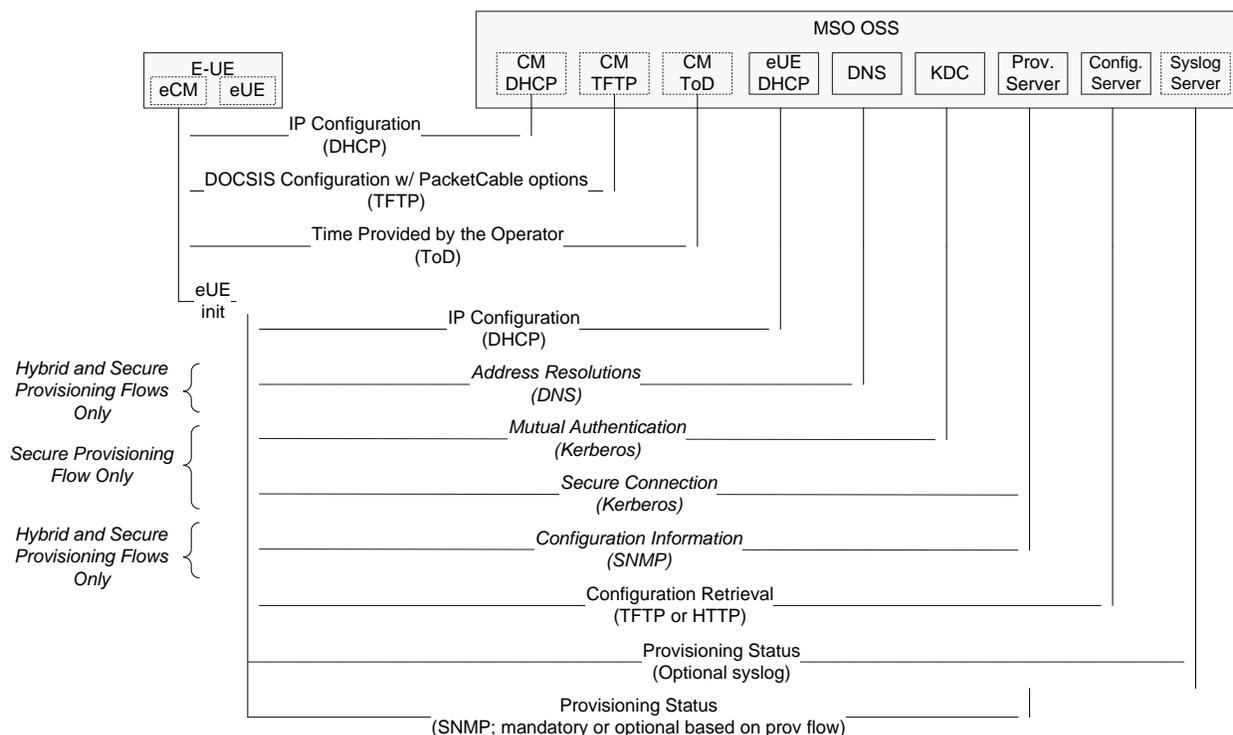
Figure 1 - PacketCable E-UE Provisioning Flow (conceptual)

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 PacketCable-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 PacketCable-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 MSO'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 PacketCable 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 specification, please refer to the PacketCable E-UE Provisioning Data Models specification [PKT-EUE-DATA].

6   E-UE PROVISIONING FRAMEWORK

This section presents the normative requirements for the E-UE Provisioning Framework, based on PacketCable 1.5 Device Provisioning. It includes references to PacketCable 1.5 Device Provisioning, and any necessary enhancements to support PacketCable E-UEs.

The framework aims to re-use all the PacketCable 1.5 Device Provisioning interfaces, and supports all three provisioning flows: Basic, Hybrid and Secure. For more information on PacketCable 1.5 Device Provisioning please refer to [PKT-PROV1.5].

Section 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 Section 6.2.1.1.

6.1   eUE Provisioning Interfaces

Figure 2 represents the network components and interfaces that form the eUE Provisioning Framework.
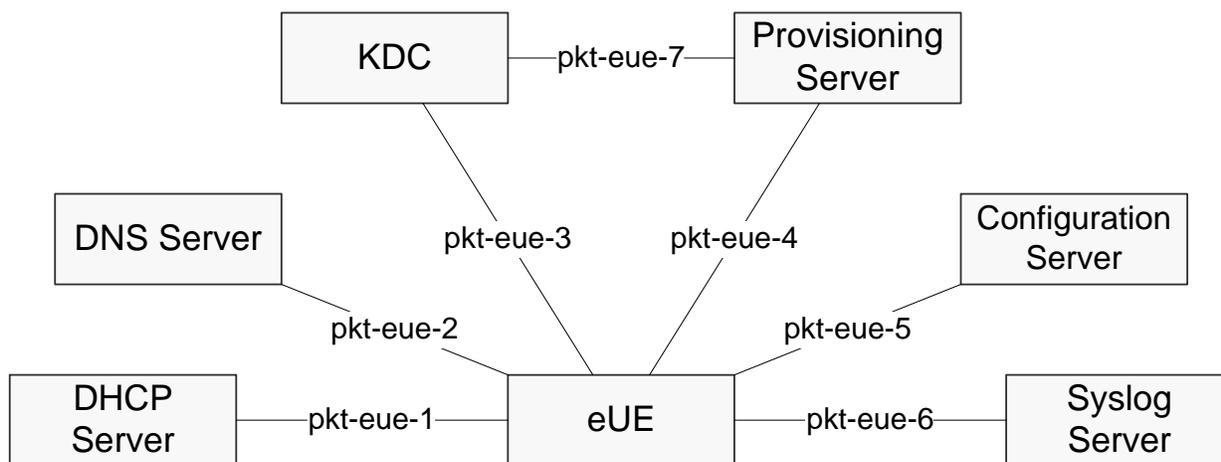
Figure 2 - E-UE Provisioning Components and Interfaces

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 PacketCable-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 document and any additional requirements specified in [RFC 2131]. 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 document and any additional requirements specified in [RFC 3315], **Error! Reference source not found.**[RFC 4861], and [RFC 4862].

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 [RFC 1034], [RFC 1035], [RFC 2782], [RFC 2915], and for IPv6 use, [RFC 3596].

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 [RFC 2234] 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 section.

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 in IPv4 addressing mode or option CL_OPTION_SYSLOG_SERVER (34) in IPv6 addressing mode). 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]. The KRB_SAFE data format within the MTA FQDN Reply, as specified in [PKT-SEC1.5], supports only IPv4 addresses and cannot support clients that support IPv6. In order to support IPv6 addresses, this document presents an alternative KRB_SAFE data format, specified in Table 1. This format also allows for clients to support multiple IP address types, i.e., IPv4 and IPv6 (simultaneously, or otherwise) and multiple IP address instances (e.g., multiple IPv6 addresses).

PacketCable Provisioning Servers deployed in networks with clients that support IPv6, or clients that can be associated with multiple IP addresses, MUST support and use the KRB_SAFE data format as specified in Table 1 (within the MTA FQDN Response Message). PacketCable KDCs deployed in networks with clients that support IPv6, or clients that can be associated with multiple IP addresses, MUST support and accept the KRB_SAFE data

format as specified in Table 1 (within the MTA FQDN Response Message). PacketCable Provisioning Servers and KDCs that support clients associated with only one IPv4 address may utilize the KRB_SAFE data format specified in [PKT-SEC1.5].

Within Table 1, all fields are in network byte order, with the most significant byte first. IPv4 and IPv6 addresses are in standard binary network form, with 4 bytes for IPv4 addresses, and 16 bytes for IPv6 addresses.

Table 1 - KRB_SAFE Data Format

Field Name	Length	Description
Message Type	1 byte	3= eUE FQDN and IP Reply
Enterprise Number	4 bytes	Network byte order, MSB first. 1 = PacketCable
Protocol Version	1 byte	2 for this version
Count of eUE IPv4 addresses	1 byte (=n1)	n1 = number of IPv4 addresses
[Sequence of eUE IPv4 addresses]	4 * n1 bytes	Zero or more eUE IPv4 addresses
Count of eUE IPv6 addresses	1 byte (=n2)	n2 = number of eUE IPv6 addresses
[Sequence of eUE IPv6 addresses]	16 * n2 bytes	Zero or more eUE IPv6 addresses
FQDN size	1 byte (=n3)	n3 = size of eUE FQDN
UE FQDN	n3	eUE FQDN

6.2   Provisioning Components

This section details the network components that utilize the interfaces specified in Section 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 document.

6.2.1   E-UE

The E-UE is a PacketCable 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 document.

The additional eCM requirements are as follows:

- The eCM component of an E-UE MUST support the PacketCable-specific DHCP options as required by the provisioning flows specified in this document.

- The eCM component of an E-UE MUST relay the PacketCable-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(es), different from the IP address(es) of the eCM.

- The eUE MUST have Dual-Stack Support (DSS).

- The eUE MUST implement Single-Stack Mode (SSM).

- The eUE MUST implement Dual-Stack Mode (DSM).

- When in SSM, the eUE MUST have a single IP address.

- When in DSM, the eUE MUST have two IP addresses: one IPv4 address and one IPv6 address (both - for the same MAC address of the eUE).

- 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(s), 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 Section 6.1 of this document.

- The eUE MUST support all three provisioning flows: Basic, Hybrid and Secure, as specified in this document, based on [PKT-PROV1.5].

- The eUE MUST support the configuration file format specified in this document and the data element definitions specified in [PKT-EUE-DATA].

- The eUE MUST support the management requirements specified in this document.

- The eUE MUST comply with all the eMTA non-data requirements specified in [PKT-PROV1.5] unless enhanced or modified in this document.

- The eUE MUST NOT use its link-local address except for protocols that explicitly require the use of the link-local address such as DHCP.

- In all other cases, where there is no explicit requirement for the use of a link-local address, the eUE MUST use its global IPv6 address. For example, the global IPv6 address is to be used for communication using protocols such as DNS, Kerberos, SNMP, TFTP, HTTP, and TLS.

6.2.2   DHCP Server

The DHCP Server is responsible for IP configuration. Within the E-UE Provisioning framework, it also supports PacketCable-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 document. 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 document.

6.2.4　KDC

The KDC is the authenticating entity for an MSO 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 document. The KDC MUST also support applicable Secure Provisioning Flow requirements, as specified in this document.

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 document.

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 document.

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 document.

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 section.

6.2.8.1　eCM DHCP Server

In addition to the DOCSIS requirements, the eCM DHCP Server MUST support the PacketCable-specific DHCP options as required by the provisioning flows specified in this document. 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 analyze 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 need 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. Similarly, this framework requires that an eUE be provisioned in such a way that it will acquire IPv4 or IPv6, or both IP addresses (DSM), 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 PacketCable-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 a PacketCable network.

The following sub-sections detail these processes and associated requirements in detail 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 document. This section 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 section. 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 PacketCable 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:			

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 Section 6.4.1 of this document 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, with the following additions (as applicable): OPTION_VI_VENDOR_OPTS(125) - CL_V4OPTION_IP_PREF(124) (value b'111) - CL_V4OPTION_ORO(1) - CL_V4OPTION_CCCV6 (123) - CL_V4OPTION_IP_PREF(124) and: OPTION-55: - CL_OPTION_CCC(122) Note: Indentation in the DHCP Options list above indicates the inclusion of the DHCP Options values.	The eCM MUST attempt IPv4 configuration with CM1.	If there is a failure in CM1, the eCM MUST behave as specified in DOCSIS.
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. The DOCSIS DHCPv4 Server MUST also include the DHCP option CL_V4OPTION_IP_PREF indicating a choice between a single (IPv4 or IPv6) or dual (IPv4 and IPv6) stack for eUE operations. 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 and 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.
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	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.

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
	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. Within this DHCP REQUEST message the eCM MUST request the same options as the corresponding DHCP DISCOVER message (CM1).		
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.
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 [CANN-DHCP-Reg] for DHCP options CL_OPTION_ORO and OPTION_VENDOR_OPTS. Refer to Section 6.4.1 of this document for DHCP options CL_OPTION_CCCV6 and CL_OPTION_IP_PREF.			

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
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: OPTION VENDOR_OPTS(17) - CL_OPTION_IP_PREF(39) (value b'111) - CL_OPTION_ORO(1) - CL_OPTION_CCCV6 (2170) - CL_OPTION_CCCV6(2171) - CL_OPTION_IP_PREF(39)	The eCM MUST attempt IPv6 configuration with CM1v6.	If there is a failure in CM1v6, the eCM MUST behave as specified in DOCSIS.
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. The DOCSIS DHCP Server MUST also include the DHCP option CL_OPTION_IP_PREF within OPTION_VENDOR_OPTS, indicating a choice between a single (IPv4, or IPV6) or dual (IPV4 and IPV6) stack for eUE operations. 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.

Flow	eCM Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
CM3v6	Upon receiving one ore 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. 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 MUST send a DHCPv6 REQUEST message. Within this DHCPv6 REQUEST message the eCM MUST request the same options as the corresponding DHCPv6 SOLICIT message (CM1v6).	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.
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 Section 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

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_CCCV6 and CL_OPTION_CCCV6 are used to request the eUE's DHCPv6 server DSS_IDs.

- DHCP options CL_V4OPTION_IP_PREF and CL_OPTION_IP_PREF are used to indicate whether or not the eUE should be operating in SSM or in DSM for most operations (e.g., media, SIP signaling). In case of provisioning operations, these DHCP options indicate if either IPv4 or IPv6 address should be used for the eUE provisioning.

eUE initialization begins with DHCP server selection. Once the eUE successfully obtains IP parameters such as IP address and the requested PacketCable options, it proceeds to select a provisioning flow. Once a provisioning flow is selected, it needs to verify if ToD has been obtained. The selection of the IP addressing mode is specified in Section 6.3.2.1. The DHCP Server Selection is specified in Section 6.3.2.2. The requirements for obtaining, and maintaining, ToD are indicated in Section 6.3.2.2.

6.3.2.1   IP Addressing Mode Selection

Table 4 indicates how the responses to an eCM's request are to be interpreted within the framework specified in this document. 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. When both DHCPv4 and DHCPv6 addresses are requested, the DHCP server indicates the IP addressing mode of provisioning by using the DHCP options CL_V4OPTION_IP_PREF and CL_OPTION_IP_PREF [CANN-DHCP-Reg]. These options, when provided to the eCM, will indicate the following IP addressing modes for eUE operations:

- **SSM**: The eUE acquires either IPv4 or IPv6 address for all its operations including Provisioning Flows. In this case, DHCP option CL_V4OPTION_IP_PREF or CL_OPTION_IP_PREF will determine the IPv4 or IPv6 address mode for eUE respectively.

- **DSM**: The eUE acquires both - IPv4 and IPv6 addresses for its operations. In addition the DHCP option CL_V4OPTION_IP_PREF or CL_OPTION_IP_PREF determines the IPv4 or IPv6 address to be used by the eUE Provisioning Flows as described in Table 4.

Table 4 - eUE Initialization and IP Addressing Mode Selection

The eCM's DHCP Server Response (DHCPv4 ACK or DHCPv6 REPLY) contains	Then the eUE initialization and IP addressing mode is determined as follows
Valid eUE DHCPv4 server address(es).	IPv4, unless explicit indicator to shutdown the eUE (see [PKT-PROV1.5]
Valid eUE DHCPv6 DSS ID(s).	IPv6, unless explicit indicator to shutdown the eUE (see Section 6.4.1).
eUE IPv4-only address acquisition mode (IP_PREF = b(value is b'001); Valid DHCPv4 server address(es) provided	IPv4, unless explicit indicator to shutdown the eUE [PKT-PROV1.5]
eUE IPv6-only address acquisition mode (IP_PREF = b(value is b'010); Valid DHCPv6; DSS ID(s) provided.	IPv6, unless explicit indicator to shutdown the eUE (see Section 6.4.1)
- Preference for eUE DHCPv4 (IP_PREF = b'101); - Valid DHCPv4 server address(es)	Dual-stack mode (IPv4 and IPv6), unless explicit indicator to shutdown as described in Section 6.3.2.2. Both IPv4 and IPv6 address acquisition will be performed.

The eCM's DHCP Server Response (DHCPv4 ACK or DHCPv6 REPLY) contains	Then the eUE initialization and IP addressing mode is determined as follows
- Valid DHCPv6; DSS ID(s)	Provisoning Operations will be performed in IPv4.
- Preference for eUE DHCPv6 (IP_PREF = b'110); - Valid DHCPv4 server address(es) - Valid DHCPv6; DSS ID(s)	Dual-stack mode (IPv4 and IPv6), unless explicit indicator to shutdown as described in Section 6.3.2.2. Both IPv4 and IPv6 address acquisition will be performed. Provisoning Operations will be performed in IPv6.
No Preference; contains valid eUE DHCPv4 server address(es)	IPv4, unless explicit indicator to shutdown the eUE [PKT-PROV1.5].
No preference; contains valid eUE DHCPv6 DSS ID(s) only	IPv6, unless explicit indicator to shutdown the eUE (see Section 6.4.1)
No preference; contains both eUE DHCPv4 server address(es) and eUE DHCPv6 server DSS_ID(s).	IPv6, unless explicit indicator to shutdown the eUE (see Section 6.4.1)
Neither eUE DHCPv4 server address(es) nor eUE DHCPv6 server DSS_ID(s)	The eUE does not attempt to provision and remains dormant until it is reinitialized by the eCM

Based on Table 4, the eUE is either initialized or disabled. If the eUE is initialized, the eCM MUST provide to the eUE corresponding DHCP server options (including option IP_PREF). When the eUE is disabled, it MUST neither initiate, nor respond to Neighbor Discovery and Router Solicitation messages.

In order to configure the eUE in a particular addressing mode, the eCM MUST use Table 5 to determine the DHCP options to be included into the DHCP message exchange.

Note that, in Table 5, the value of b'111 of the DHCP Options CL_V4OPTOIN_IP_PREF and CL_OPTION_IP_PREF is used by the eCM to indicate the eUE dual stack support to the Back-office Provisioning System.

Table 5 - DHCP Options used by eCM for eUE Configuration

eCM is in	eCM DHCP Exchange Requirement

IPv4 Addressing Mode	CM DHCPv4 DISCOVER message MUST include the following:
	
	 OPTION_VI_VENDOR_OPTS(125)
	
	     - CL_V4OPTION_IP_PREF(124) (value b'111)
	
	     - CL_V4OPTION_ORO(1)
	
	        - CL_V4OPTION_CCCV6 (123)
	
	        - CL_V4OPTION_IP_PREF(124)
	
	 and:
	
	 OPTION-55:
	
	     - CL_OPTION_CCC(122)

eCM is in	eCM DHCP Exchange Requirement
IPv6 Addressing Mode	CM DHCPv6 SOLICIT message MUST include the following: OPTION_VENDOR_OPTS(17): - CL_OPTION_IP_PREF(39) (value b'111) - CL_OPTION_ORO(1) - CL_OPTION_CCC (2170) - CL_OPTION_CCCV6(2171) - CL_OPTION_IP_PREF(39)

6.3.2.2   DHCP Server Selection

An eUE provisioning in IPv4 mode performs DHCPv4 server selection as specified in [PKT-PROV1.5]. The eCM is provided with a primary, and optionally secondary, DHCPv4 server address via sub options 1 and 2 within DHCPv4 option 122 (eCM provisions in IPv4 mode) or DHCPv6 option CL_OPTION_CCC (eCM provisions in IPv6 mode). The eCM passes this information onto the eUE. The eUE filters the DHCPv4 OFFER messages it receives, and accepts a DHCPv4 OFFER from a server whose server-identifier matches the primary or secondary DHCPv4 addresses, and provides the necessary DHCP parameters. It is to be noted that a value of 255.255.255.255 for the DHCPv4 server address directs the eUE to accept a valid DHCPv4 OFFER from any server. Similarly, a value of 0.0.0.0 indicates that the eUE must not provision.

A eUE provisioning in IPv6 mode performs DHCPv6 server selection in a manner similar to the DHCPv4 server selection. However, DHCPv6 messages do not contain DHCPv6 server addresses. To provide server identification in DHCPv6, we use the CableLabs-specific DHCP Server Selection Identifier (DSS_ID). The eCM is provided with a primary, and optionally secondary, DSS_ID via sub options 1 and 2 within DHCPv4 option CL_V4OPTION_CCCV6 (eCM provisions in IPv4 mode), or DHCPv6 option CL_OPTION_CCCV6 (eCM provisions in IPv6 mode). The eCM passes this information onto the eUE. When a PacketCable 2.0 DHCPv6 server responds with a DHCPv6 ADVERTISE message, in response to a DHCPv6 SOLICIT message from an eUE, it includes its DSS_ID within sub-option 1 of CL_OPTION_CCC. Note that a DHCPv6 server responding with a DHCPv6 ADVERTISE to the eUE will not include sub-option 2 within CL_OPTION_CCCV6. If sub-option 2 is included within CL_OPTION_CCCV6 the eUE will ignore it. The eUE must only accept valid DHCPv6 ADVERTISE messages from servers supplying a DSS_ID matching one of the two eCM-provided DSS_IDs (or the sole eCM-provided DSSID when only the eCM was given only one). If the eCM obtained a value of 0xFF 0xFF 0xFF 0xFF (four all-ones octets) in sub-option 1 of CL_V4OPTION_CCCV6 or CL_OPTION_CCCV6, then the eUE is free to accept a valid DHCPv6 Advertise from any server, regardless of that server's DSSID. Similarly, a value of 0x00 0x00 0x00 0x00 (four zero-valued octets) indicates that the eUE must not provision.

An eUE provisioning in DSM, performs the DHCPv4 and DHCPv6 servers selection as described above in this section for both – IPv4 and IPv6 modes. In addition, if either of the DHCP servers (DHCPv4 or DHCPv6) indicates that the eUE should not proceed with provisioning (as described in this section), the eUE MUST NOT provision.

6.3.2.3   Obtaining and Maintaining ToD

The DOCSIS specifications allow the CM component to obtain the time from the Time Of Day (ToD) Server, after suitable retries, if required. This time is then used by the UE for provisioning and management operations such as the Kerberos message flows and management event notifications.

The DOCSIS specifications, however, can allow for the CM to obtain its configuration and become operational in the absence of time from the ToD server. In such cases, it can affect certain MTA operations, specifically the secure provisioning flow.

When the DOCSIS specifications allow a CM to register and become operational, i.e., successful completion of all the mandatory steps from CM1-CM10 or CM1v6-CM10v6, and it has not yet obtained the time after an iteration of a DOCSIS (required or recommended) retry process, the UE MUST initiate provisioning via the DHCP process. In such cases, i.e., the UE has not obtained the time from the CM, the following requirements apply:

- If the eUE DHCP process indicates the Secure Provisioning flow for the eUE, then the eUE MUST NOT proceed with further Provisioning steps beyond the DHCP process. Along with that, the eEU MUST retry the initialization stage (i.e., eUE-1) periodically at least once and no more than three times per 300-second interval. After the correct ToD value is retrieved, the eUE MUST continue with the corresponding Provisioning Flow beyond the DHCP Process. As an illustration, in case of the exponential binary backoff algorithm, three consecutive retries of the DHCP Process may be separated by 30, 60, and 120 seconds intervals.

- If the eUE DHCP process indicates the basic or hybrid provisioning flows, then the eUE MUST continue with the provisioning attempt.

- In either case, the eUE MUST acquire the ToD from eCM at the moment when the ToD is successfully retrieved by the eCM. Note that, in case of Basic or Hybrid Provisioning flows, the latter may happen after the entire eUE provisioning is complete.

Each time the eUE successfully completes its DHCP Process, and in cases when the time has not been retrieved by the eCM, the eUE MUST generate the corresponding management event specified in [PKT-EUE-DATA].

Whenever there is a change in the value of the ToD DHCP Option as a result of the eCM DHCP message exchange, the eCM MUST immediately initiate the retrieval of the ToD value from the new ToD servers. In case of the ToD Server response failure, the eCM MUST periodically retry its attempts until it succeeds (as described in [DOCSIS-MULPI]).

Upon successful retrieval of a new Time of Day value, or whenever there is a change in the value of the Time Offset DHCP Option during the eCM DHCP message exchange, the eCM MUST immediately calculate the new Time of Day value based on the new ToD Server response and/or on a new value of the Time Offset.

Whenever the new ToD value is calculated by the eCM, the eUE MUST immediately use the new Time of Day value in all further operations where Time of the Day is required (e.g., Kerberos operations, event messages). If an eUE is operating in Secure Provisioning Flow, it MUST invalidate all Kerberos tickets (per [PKT-SEC1.5]). In addition, an eUE MUST generate the corresponding management event specified in [PKT-EUE-DATA]

In addition, as the eCM component is not capable of providing the IP transport until the CM10 (or CM10v6) is successfully complete (registration with the CMTS), the eUE MUST NOT initiate its DHCP Process before the successful completion of the CM10 (or CM10v6).

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], "Embedded-MTA Secure Power-on Initialization Flow (IPv4 eCM) section." An eUE initialized in Pv4 addressing mode MUST also comply with [RFC 4361]. This will allow for the consistent identification of an eUE, irrespective of whether it is provisioned in IPv4 or IPv6 modes. The eUE SHOULD include the TFTP Blocksize option [RFC 2348] when requesting the configuration file. If the eUE supports the TFTP Blocksize option, the eUE MUST request a blocksize of 1448 when using TFTP over IPv4.

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 sub-sections.

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[RFC 4862].

- The eUE MUST use the EUI-64 (64-bit Extended Unique Identifier) as a link-local address for its management interface as described in [RFC 3513].

- The eUE MUST use Duplicate Address Detection (DAD), as described in [RFC 4862], 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 EUE-EV-12 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 [RFC 4861], 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 [RFC 4861].

- 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 report the event EUE-EV-13 in its local log and 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 6 - eUE Provisioning Flow for IPv6 Addressing. The eUE MUST NOT use DHCPv6 Rapid Commit during this flow.
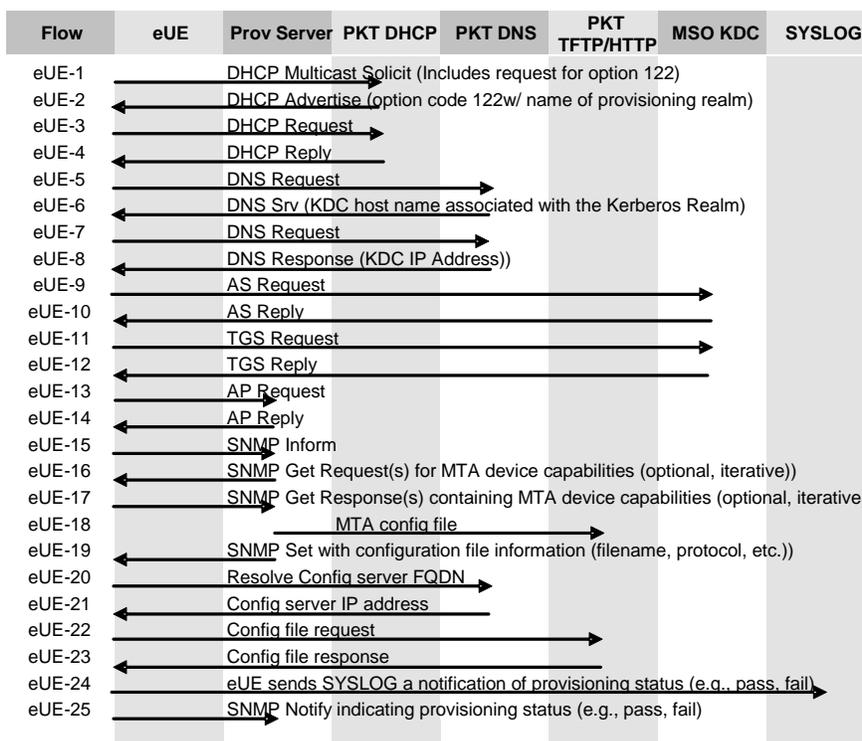
Flow	eUE	Prov Server	PKT DHCP	PKT DNS	PKT TFTP/HTTP	MSO KDC	SYSLOG
eUE-1	DHCP Multicast Solicit (Includes request for option 122)						
eUE-2	DHCP Advertise (option code 122w/ name of provisioning realm)						
eUE-3	DHCP Request						
eUE-4	DHCP Reply						
eUE-5	DNS Request						
eUE-6	DNS Srv (KDC host name associated with the Kerberos Realm)						
eUE-7	DNS Request						
eUE-8	DNS Response (KDC IP Address))						
eUE-9	AS Request						
eUE-10	AS Reply						
eUE-11	TGS Request						
eUE-12	TGS Reply						
eUE-13	AP Request						
eUE-14	AP Reply						
eUE-15	SNMP Inform						
eUE-16	SNMP Get Request(s) for MTA device capabilities (optional, iterative))						
eUE-17	SNMP Get Response(s) containing MTA device capabilities (optional, iterative)						
eUE-18	MTA config file						
eUE-19	SNMP Set with configuration file information (filename, protocol, etc.))						
eUE-20	Resolve Config server FQDN						
eUE-21	Config server IP address						
eUE-22	Config file request						
eUE-23	Config file response						
eUE-24	eUE sends SYSLOG a notification of provisioning status (e.g., pass, fail)						
eUE-25	SNMP Notify indicating provisioning status (e.g., pass, fail)						

Figure 3 - eUE Provisioning Flow in IPv6 Addressing Mode

Table 6 - 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 [CANN-DHCP-Reg] for DHCP option CL_OPTION_MODEM_CAPABILITIES. Refer to Section 6.4.1 of this document for DHCP option CL_OPTION_CCCV6.			
eUE-1	DHCPv6 SOLICIT Message The eUE MUST send a multicast DHCPv6 SOLICIT message that includes the following options: - **OPTION_CLIENTID(1)** containing the DUID (DHCP Unique Identifier) for the eUE, as specified by [RFC 3315]. The eUE can choose any one of the rules to construct the DUID according to [RFC 3315], section 9.1; - **OPTION_ IA_NA(3)** (Identity Association for Non-temporary Addresses) to obtain an IPv6 address assignment. - **OPTION_FQDN(39)** (Client FQDN Option as per [RFC 4704]) containing an empty "domain name" field, and containing a "flags" field with flag values S=1, N=0, O=0. - **OPTION_ORO(6)** requesting the following standard options from the server:	The eUE MUST NOT proceed to eUE-1 prior to successful completion of either CM10 or CM10v6.	If failure per DHCP protocol, the eUE MUST repeat eUE-1.

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
	- OPTION_FQDN(39), [RFC 4704])		
	- OPTION_DNS_SERVERS(23)OPTION_VENDOR_OPTS(17)		
	- **OPTION_VENDOR_CLASS (16)** containing enterprise number 4491 and the string "pktc2.0".		
	- **OPTION_VENDOR_OPTS (17)** containing enterprise number 4491, and further containing the following CableLabs vendor options:		
	- CL_OPTION_DEVICE_TYPE(2) with the name identifying the EUE device as defined in [CANN-DHCP-Reg].		
	- CL_OPTION_DEVICE_SERIAL_NUMBER(4) with the EUE embedded device serial number as defined in [CANN-DHCP-Reg].		
	- CL_OPTION_HARDWARE_VERSION_NUMBER(5) as defined in [CANN-DHCP-Reg].		
	- CL_OPTION_SOFTWARE_VERSION_NUMBER(6) as defined in [CANN-DHCP-Reg].		
	- CL_OPTION_BOOT_ROM_VERSION(7) as defined in [CANN-DHCP-Reg].		
	- CL_OPTION_VENDOR_OUI(8) as defined in [CANN-DHCP-Reg].		
	- CL_OPTION_MODEL_NUMBER(9) as defined in [CANN-DHCP-Reg].		
	- CL_OPTION_VENDOR_NAME(10) as defined in [CANN-DHCP-Reg].		
	- CL_OPTION_MODEM_CAPABILITIES(35), with the formatting specified in [CANN-DHCP-Reg] and the content specified in the Section 6.6.1 of this document.		
	- CL_OPTION_DEVICE_ID(36) containing eUE MAC address		
	CL_OPTION_CORRELATION_ID(2172) containing correlation ID - CL_OPTION_ORO(1) requesting the following vendor specific options from the server:		
	- CL_OPTION_TFTP_SERVERS(32) as defined in [CANN-DHCP-Reg]		
	- CL_OPTION_CONFIG_FILE_NAME(33) as defined in [CANN-DHCP-Reg]		
	- CL_OPTION_SYSLOG_SERVERS(34) as defined in [CANN-DHCP-Reg]		
	- CL_OPTION_CCCV6(2171) as defined in [CANN-DHCP-Reg]		

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
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 Section 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 [RFC 3315].	If failure per DHCP protocol, the eUE MUST restart with eUE-1.
eUE-3	DHCPv6 REQUEST Message After sending the DHCP SOLICIT message, the eUE MUST await valid DHCP ADVERTISE messages as specified in [RFC 3315]. A valid DHCP ADVERTISE MUST contain CL_OPTION_CCCV6 with valid sub-options 1, 3 and 6, where sub-option 1 identifies that it originates from an allowed DHCP server (as indicated by the eCM). 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 seven-byte ASCII string "0.0.0.0". 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 "0.0.0.0" 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 "0.0.0.0" 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. Within this DHCPv6 REQUEST message the eUE MUST request the same options as the corresponding DHCPv6 SOLICIT message (eUE-1).	The eUE DHCP Server MUST NOT proceed with eUE-3 before waiting for eUE-2 to complete, as indicated by [RFC 3315].	If failure per DHCP protocol, the eUE MUST restart with eUE-1.
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).	The eUE DHCP Server MUST NOT proceed with eUE-4 before successful completion of eUE-3, per [RFC 3315].	If failure per DHCP protocol, the eUE MUST return to eUE-1.

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
	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 ([RFC 4862]) 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 MUST also report the event EUE-EV-12 in its local log.		
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], section 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], section 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.
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].

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
NOTES: 1. Flows eUE-11 and eUE-12 below are optional in some cases. Refer to [PKT-SEC1.5] for more information. 2. SNMPv3 entity (FQDN) MUST be resolved to an IP address anywhere during flows eUE-5 to eUE-12. 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].
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.			

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 PacketCable. 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 NOT include the last MIB Object to the SNMPv3 varbinding if the eUE Configuration File is not encrypted. The eUE MUST respond to a valid SNMP SET operation, per SNMP protocol. NOTES: 1. In the case of file download using the HTTP access method, the filename MUST be URL-encoded with a URL format compliant with [RFC 2616] with exception stated below in NOTE 3 below. 2. In the case of file download using the TFTP access method, the filename MUST be URL-encoded with a URL format compliant with [RFC 3617] with	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.

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
	the exception stated in NOTE 3 below. 3. The eUE MUST accept IPv6 addresses in colon separated format embedded in a URL; refer to [RFC 4291] for IPv6 address encoding, and [RFC 3986] for the encoding of an IPv6 address in URL format.		
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 [RFC 1350] – for TFTP and [RFC 2616] – for HTTP respectively. The eUE MUST include the TFTP Blocksize option [RFC 2348] when requesting the configuration file via TFTP. The eUE MUST request a blocksize of 1428 when using TFTP over IPv6. When a eUE is provisioning using BASIC Provisioning Flow to obtain the configuration file using IPv6, and it is provided with multiple TFTP Server IP addresses within DHCPv6, the eUE MUST follow the backoff, retry and failure mechanisms as specified in the DOCSIS MULPI specification [DOCSIS-MULPI]. Refer to the section titled "Transfer Operational Parameters" within [DOCSIS-MULPI] that describes CM backoff, retry, and failure behavior in the presence of multiple TFTP servers when using IPv6. If the eUE recognizes IP connectivity failure, as specified in the referenced section within [DOCSIS-MULPI], then the eUE MUST retry provisioning.	The eUE MUST peform 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.
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 [RFC 1350] – for TFTP and [RFC 2616] – 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 has calculation are provided in [PKT-SEC1.5]. Refer to Section 6.4.2 of this document 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	The eUE MUST peform eUE-24 after eUE-23 is completed, if	If a failure is detected, the eUE MAY retry this step before proceeding

Flow	eUE Power-On Initialization Flow Description	Normal Flow Sequence	Sequence upon failure of a Flow Step
	SYSLOG a "provisioning complete" event indicating the status of the provisioning operation. This notification will include the pass-fail result of the provisioning operation.	SYSLOG is configured.	to eUE-25.
eUE-25	SNMP INFORM The eUE MUST send the PROV_SNMP_ENTITY, specified within sub-option 3 of DHCP CL_OPTION_CCCV6(2171), an SNMP INFORM containing a "provisioning complete" notification. The receipt of the inform is acknowledged by the response message as defined in [RFC 3414]. 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   eUE Provisioning for Dual Stack Mode

As established in the previous paragraphs, and depending on the value of the DHCP Option IP_PREF, an eUE can be either in a single or a dual stack mode. In DSM, an eUE MUST acquire two IP addresses for its MAC Address:

- primary IP address - for Provisioning, Management, and potentially for signaling and Media (RTP/RTCP).

- secondary IP address - potentially for signaling and Media, but never for Provisioning, Management.

The eUE MUST acquire its primary IP address during the Provisioning process as described in the previous sections of the document.   The type of the primary IP address in DSM is determined by the value of IP_PREF (per [CANN-DHCP-Reg].

The eUE MUST choose its secondary IP address type to be complementary to the primary one: if the primary address is of IPv4 type, then the secondary address type will be of IPv6 type and vice-versa.

The determination of the IP address used for media is done by the procedures defined in [PKT-24.229]. Note that these procedures may determine either - the primary or the secondary IP address of the eUE to be used for media.

An eUE MUST attempt to acquire a secondary IP address before it reaches provisioning state of "pass" or "passwithwarning". The secondary address acquisition is not considered to be a part of the eUE Provisioning process. Therefore, in case of a failure to acquire the secondary IP address before the Provisioning Flow is completed, an eUE MUST NOT indicate the "Provisioning failure" of the eUE Provisioning.

Note that it is highly recommended that the acquisition of the primary and secondary addresses in DSM be performed as two concurrent processes. However, it maybe sub-optimal to acquire a secondary IP address prior to successful acquisition of the primary IP Address or credentials validation (e.g., MTA15, eUE-15).

Figure 4 depicts the overall logic of the eUE Provisioning in DSM.
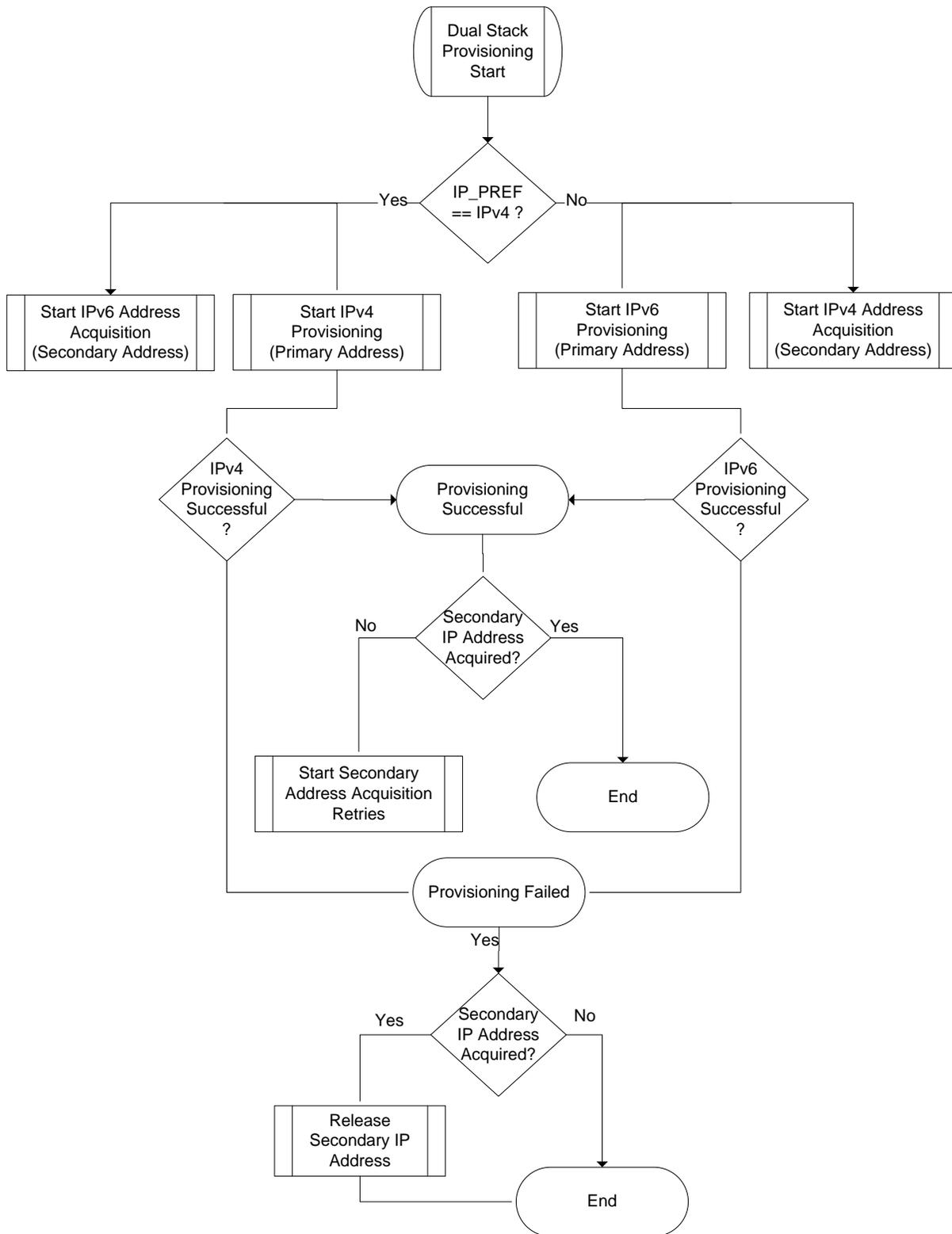
Figure 4 - Provisioning Logic in Dual Stack Mode.

Note: On Figure 4 the "Provisioning Failed" state corresponds to any of the following results of the eUE
        Provisioning: "failConfigFileError", "failureInternalError", or "failOtherReason" as defined in the
        "pktcMtaDevProvisioningState" MIB Object [PKT-EUE-DATA].

6.3.5.1   IPv4 Secondary Address Acquisition

To acquire the secondary IPv4 address, the eUE MUST follow the requirements described in the Provisioning Flows MTA1 thru MTA4 [PKT-PROV1.5], with the following exceptions:

- The eUE MUST use at least the following DHCPv4 options: Option 60 and Option 43 as described in [PKT-PROV1.5].

- Once the DHCPv4 OFFERs are collected, the eUE MUST choose the DHCPv4 server, that is pointed to by the eCM DHCPv4 Option-122 as described in [PKT-PROV1.5].

- If the eCM obtained a value of 255.255.255.255 in sub-option 1 of the Option-122, then eUE can use any valid DHCPv4 OFFER message from any DHCPv4 server.Similarly, a value of 0.0.0.0 indicates that eUE MUST NOT acquire a secondary IP address.

- An eUE MUST ignore all PacketCable 2.0 DHCPv4 Options which it may potentially receive during the DHCPv4 message exchange with the DHCPv4 server(s).

- For any DHCPv4 message, the eUE MUST follow the retransmission requirements as stated in [RFC 2131].

- In case of a failure of any DHCP step per DHCPv4 protocol, the eUE MUST start the secondary IP address acquisition anew (sending the DHCPDISCOVER) message. Along with that, the eUE MUST report the PROV-EV-16 management event message [PKT-MEM1.5].

6.3.5.2   IPv6 Secondary Address Acquisition

Before acquiring the IPv6 secondary address, the eUE MUST first acquire the Link-local address (as described in Section 6.3.4.1), followed by the Router Discovery procedure (as described in Section 6.3.4.2). In case of failure of the Router Discovery procedure, the eUE MUST proceed as if the secondary IP address acquisition has failed as described in Section 6.3.5.3. Also note that in this situation the eUE will operate as a SSM device.

The eUE MUST perform the IPv6 address acquisition if, and only if, the Link-Local address and Router Discovery procedures are successful.

To acquire the secondary IPv6 address, the eUE MUST follow the requirements described in the Section 6.3.4.3 for the Provisioning Flows eUE-1 through eUE-4 with the following exceptions:

- An eUE MUST use at least the following DHCPv6 options in DHCPv6 messages: OPTION_CLIENTID, OPTION_IA_NA, and OPTION_VENDOR_OPTS with all corresponding CableLabs vendor options (as described in Table 8), except for CL_OPTION_ORO.

- Once the DHCPv6 ADVERTISE messages are collected, the eUE MUST choose the DHCPv6 server as described in Section 6.3.2.2.

- If the eCM obtained a value of 0xFF 0xFF 0xFF 0xFF (four all-ones octets) in sub-option 1of CL_V4OPTION_CCCV6 or CL_OPTION_CCCV6, then the eUE can use any valid DHCPv6 ADVERTISE message from any DHCPv6 server. Similarly, a value of 0x00 0x00 0x00 0x00 (four all-zeros octets) indicates that eUE MUST NOT acquire a secondary IP address.

- An eUE MUST ignore all PacketCable 2.0 DHCPv6 Options which it may potentially receive during the DHCPv6 message exchange with the DHCPv6 server(s).

- For any DHCPv6 message, the eUE MUST follow the retransmission requirements as stated in [RFC 3315].

- In case of failure of any DHCP step per DHCPv6 protocol, the eUE MUST start the second IP address acquisition anew (sending DHCPSOLICIT message). Along with that, the eUE MUST report the PROV-EV-16 management event message in the local log [PKT-EUE-DATA].

6.3.5.3   Common Secondary Address Acquisition Requirements

As described previously, the eUE may encounter failures at particular DHCP stages. However, it may also happen that after performing all required DHCP message retransmissions for a failed DHCP stage, the eUE will still be unable to acquire the IP address. In such cases, the eUE MUST re-try the entire process of the secondary address acquisition until either this process succeeds or until Secondary Address Acquisition Timer (SAAT) expired, whichever happens first. The eUE MUST use the value of SAAT equal to the value of the "Provisioning Timer" [PKT-PROV1.5]. Note that the SAAT is a different timer than "Provisioning Timer", it just uses the same value. An eUE MUST start SAAT upon starting a very first attempt to acquire the secondary DHCP address (very first DHCPDISCOVER or DHCPSOLICIT message). An eUE MUST stop SAAT either when the secondary IP address acquisition is successfully acquired or when the SAAT expires. The latter condition is considered to be the "secondary address acquisition failure". In case of secondary address acquisition failure, the eUE MUST stop all further attempts to acquire the secondary address until reset.

Upon the secondary IP address acquisition failure, the eUE MUST report the Management Event message "EUE-EV-14" [PKT-EUE-DATA] to signal the failure to the backoffice.

Upon successful acquisition of the secondary IP address, the eUE MUST use the Management Event message "EUE-EV-15" [PKT-EUE-DATA] to signal the success to the backoffice.

Once the secondary IP address is acquired, the eUE MUST follow the requirements of the IPv4 or IPv6 DHCP protocol (whichever is applicable to the secondary IP address).

Upon the successful acquisition of the secondary IP address, the eUE MUST populate the "ipNetToPhysicalTable" MIB Objects as required by [RFC 4293].

In case the eUE Provisioning Process results in any of the Provisioning states "failConfigFileError", "failureInternalError", or "failOtherReason", the eUE MUST immediately release the secondary IP address in case it has been acquired.

6.3.6   Post-Initialization DHCP Behavior

It is possible that, during the DHCPv4 and DHCPv6 lease renewal operations, the eUE will receive updated fields in DHCP server response messages.

In the case of DHCPv4:

- If the IP address (yiaddr) value is different in the DHCPACK response than the current value used by the eUE, the eUE MUST reinitialize and start from eUE-1;

- If the subnet mask (option 1) or the next-hop router (option 3) values are different in the DHCPACK response than the current values used by the eUE, the eUE MAY either use the new values (if possible) without reinitializing, or reinitialize and start from eUE-1;

- If the DNS servers (option 6) or the SYSLOG server addresses (option 7) in the DHCPACK is different than the servers currently in use, the eUE MUST use the new values for all future operations without reinitializing, including reporting via management;

- For other configuration options, the eUE MUST ignore any differences between the currently used values and values in renewal DHCPACK responses. This includes the 'file' and 'siaddr' fields (only used in Basic Provisioning Flow), hostname (option 12), domain name (option 15), and all sub-options of CableLabs Client Configuration (option 122).

In the case of DHCPv6:

- If the eUE Management Address (IPv6 address field of the IA Address option, within the IA_NA option) is different in the DHCP REPLY than the current value used by the eUE, the eUE MUST reinitialize and start from eUE-1;

- If the DNS servers (option 23) or the SYSLOG servers (CL_OPTION_SYSLOG_SERVERS) in the DHCP REPLY is different than the servers currently in use, the eUE MUST use the new values for all future operations without reinitializing, including reporting via management;

- For other configuration options, the eUE MUST ignore any difference between the currently used values and values in the renewal DHCP REPLY messages. This includes CL_OPTION_TFTP_SERVERS and CL_OPTION_CONFIG_FILE_NAME (only used in Basic Provisioning Flow), Reconfigure Accept (option 20), the FQDN option (option 39), and all sub-options of CL_OPTION_CCCV6).

Additionally, in DHCPv6 RENEW/REBIND messages, the eUE MUST send its last known FQDN in the 'domain name' field of OPTION_FQDN.

6.3.7   Post-Initialization Incremental Provisioning

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

PacketCable 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 Section 6.3 of this document, using DHCP. To facilitate this, certain E-UE Provisioning specific DHCP options were utilized that are summarized in the following sub-sections. 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 [RFC 3925] and [RFC 3315], 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. The E-UE MUST be capable of retrieving and processing the data contained in all of the "required" and "optional" sub-options defined in [PKT-PROV1.5]. Additionally, values for shutting down the eUE component in DHCPv4 mode 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 [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 eCM that obtains a DSS_ID that is longer MUST only consider the first 32 bytes. Two distinguished DSS_ID values are reserved within DHCP option CL_V4OPTION_CCCV6: the DSS_ID consisting of exactly four zero-valued octets (0x00, 0x00, 0x00, 0x00), and the DSS_ID consisting of exactly four all-ones octets (0xFF, 0xFF, 0xFF, 0xFF). The eCM MUST interpret the reserved values of the DSS_ID in the same manner as the IPv4 address values "0.0.0.0" and "255.255.255.255", respectively, in option 122, sub-option 1. The DHCPv6 Server MUST include sub-option 1 in the DHCP OFFER/ACK to the eCM, where it indicates the Primary DHCPv6 server's DSS_ID.

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 [CANN-DHCP-Reg].

6.4.1.4   DHCP Option CL_OPTION_CCCV6

This CableLabs-specific DHCP option is used by PacketCable compliant devices to obtain PacketCable-specific configuration during the IP address acquisition phase. It is specified in [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.

Two distinguished DSS_ID values are reserved within DHCP option CL_OPTION_CCCV6: the DSS_ID consisting of exactly four zero-valued octets (0x00, 0x00, 0x00, 0x00), and the DSS_ID consisting of exactly four all-ones octets (0xFF, 0xFF, 0xFF, 0xFF). The eCM MUST interpret the reserved values of the DSS_ID in the same manner as the IPv4 address values "0.0.0.0" and "255.255.255.255", respectively, in option 122, sub-option 1.

The DHCP Server MUST include sub-option 1 in the DHCPv6 ADVERTISE/REPLY to the eCM, where it indicates the Primary DHCPv6 server's DSS_ID. A DHCPv6 server responding with a DHCPv6 ADVERTISE to the eUE MUST NOT include sub-option 2 within CL_OPTION_CCCV6. When identifying the advertising server in its DHCP transaction, the eUE MUST only consider the value for DSS_ID that is present in sub-option 1. If sub-option 2 is present, then the eUE MUST ignore it. The DHCP Server MUST include sub-option 1 in the DHCPv6 ADVERTISE/REPLY to the eUE, where it indicates the identity of the responding DHCPv6 server.

6.4.1.5   DHCP Option CL_V4OPTION_IP_PREF

For a DSS capable eUE, when the eCM is operating in IPv4 mode and the eUE requests both DHCPv4 server option and DHCPv6 server option, the eCM's DHCP server MUST use the DHCP Option CL_V4OPTION_IP_PREF to indicate a preference. This DHCP option is specified in [CANN-DHCP-Reg].

The eUE MUST send the value of b'111 to the DHCPv4 server in CL_V4OPTION_IP_PREF DHCP Option to indicate its DSS capabilities to the DHCP server.

6.4.1.6   DHCP Option CL_OPTION_IP_PREF

For a DSS capable eUE, when the eCM is operating in IPv6 mode and the eUE requests DHCPv4 server option and DHCPv6 server option,the eCM's DHCP server MUST use the DHCP Option CL_OPTION_IP_PREF to indicate a preference. This DHCP option is specified in [CANN-DHCP-Reg].

The eUE MUST send the value of b'111 to the DHCPv6 server in CL_OPTION_IP_PREF DHCP Option to indicate its DSS capabilities to the DHCP server.

6.4.1.7   DHCP Option CL_OPTION_CORRELATION_ID

The correlation ID is a random value generated by the eUE after a software reset or hard reboot. This value is communicated by the eUE to Provisioning Application as part of the device capability data. Correlation ID is used as an identifier to correlate related events in the eUE provisioning sequence. When a eUE is operating in IPv6 mode, the DHCPv6 message has to be populated with correlation ID using the CL_OPTION_CORRELATION_ID. This value MUST be identical to the content of the pktcMtaDevCorrelationId MIB object. This DHCP option is specified in [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.

PacketCable configuration data required for the eUE to communicate with a PacketCable network such as device-level, user-level and application-level data is provided via the eUE configuration file. This section 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 triplet uniquely identifies the particular data item being provisioned via the Configuration File. Table 7 contains the TLV Types used for PacketCable eUE Configuration File and requirements on using them.

Table 7 - 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 with one exception: The sub-option 8 contains the Organizational Unique Identifier (OUI) represented as a ascii-encoded 6-byte octet string. All other MTA requirements in [PKT-PROV1.5] apply.
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 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 Section 6.5 of this document.
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 MUST implement all the TLV types described in Table 7. The eUE MUST also follow the applicable requirements described in [PKT-PROV1.5], section titled "MTA Configuration File," for processing the configuration file data, with one exception related to row creation of the MIB Tables. An eUE MUST comply with the requirements specified in [RFC 2579] for row creation within MIB tables when tabular data is provided in the configuration file. Specifically, the eUE MUST support 'CreateAndGo' for row creation, as specified in [RFC 2579]. The eUE MAY also support 'CreateAndWait', as specified in [RFC 2579]. If an eUE does not support 'CreateAndWait' for row creation and it receives the 'CreateAndWait' directive within the configuration file, the eUE MUST consider this as a configuration file error (failConfigFileError) and report it in accordance with the requirements of [PKT-PROV1.5] (i.e., within the error oids MIB table). When a table row creation is requested in the configuration file and the required row status MIB object is absent, the eUE MUST reject such row create entries, report the appropriate error code based on the table entries (e.g., 'passWithWarnings', 'failConfigFileError'), and identify such entries in the error oids MIB table.

The Provisioning Server MUST support all the TLV types described in Table 6, and follow the applicable requirements described in [PKT-PROV1.5], section titled "MTA Configuration File", for creating configuration file data. The Provisioning Server MUST also comply with the requirements specified in [RFC 2579] for MIB table row creation when providing tabular data within a configuration file.

6.4.2.1   Device Level Configuration Data

The eUE MUST follow the requirements described in [PKT-PROV1.5], section 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 7);

- the "Telephony Config File End" attribute will be interpreted as the "eUE End of File" attribute (as in Table 7);

- the applicable eUE MIBs are specified in [PKT-EUE-DATA];

- unlike [PKT-PROV1.5], the MIB object 'pktcMtaDevRealmName' is not an index and needs to be included explicitly in the configuration file. Thus, the Provisioning Server MUST include the MIB object 'pktcMtaDevRealmName' and the associated realm organization name MIB object ('pktcMtaDevRealmOrgName'), within the same conceptual row, in the configuration file when Secure Provisioning Flow is used. If the eUE does not receive both of these MIB objects for the same conceptual row during the Secure Provisioning Flow, the eUE MUST treat it the same way as the absence of the MIB object 'pktcMtaDevRealmOrgName' in [PKT-PROV1.5]. When these MIB objects are present, the eUE MUST adhere to the requirements specified in [PKT-PROV1.5] to ensure that the realm name and realm organization name match what was received during the secure provisioning flow, within DHCP and Kerberized SNMPv3 messages, respectively.

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 document.

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], section 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 MSO's OSS. To facilitate this behavior, the framework specified in this document 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], section 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(35) DHCPv6 option specified in [CANN-DHCP-Reg], and will use the DHCPv6 option OPTION_VENDOR_CLASS (16) with the CableLabs enterprise number (4491) and the string "pktc2.0" to transport the capabilities data to the DHCP server. The capabilities data is sent to the server as specified in Table 6 of this document.

- The capabilities to be reported are specified in Annex A.

- PacketCable 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.

PacketCable 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].

6.6.5   Certificate Bootstrapping

E-UEs need to be configured with IMS credentials to register and communicate with a PacketCable 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.

Certificate Bootstrapping refers to the processes by which an eUE containing, and presenting, a PacketCable defined X.509 certificate can be provided with alternative credentials to enable participation in a PacketCable network. The association between the eUE certificate and alternative credentials to be provided is Operator specific and is out of scope for this specification.

Certificate Bootstrapping involves the establishment of a secure communication interface between the eUE and a Certificate Bootstrapping Server, via which the eUE obtains the necessary credentials. The communication protocol used is HTTP, secured via TLS. The credentials are provided via an XML Schema specified in [PKT-EUE-DATA].

The process is initiated using management data elements. This process is provided as a recommended alternative to secure credential delivery via the secure provisioning flow and SNMPv3 management.

An eUE SHOULD support Certificate Bootstrapping. An eUE that supports Certificate Bootstrapping MUST follow the flow depicted in Figure 5.
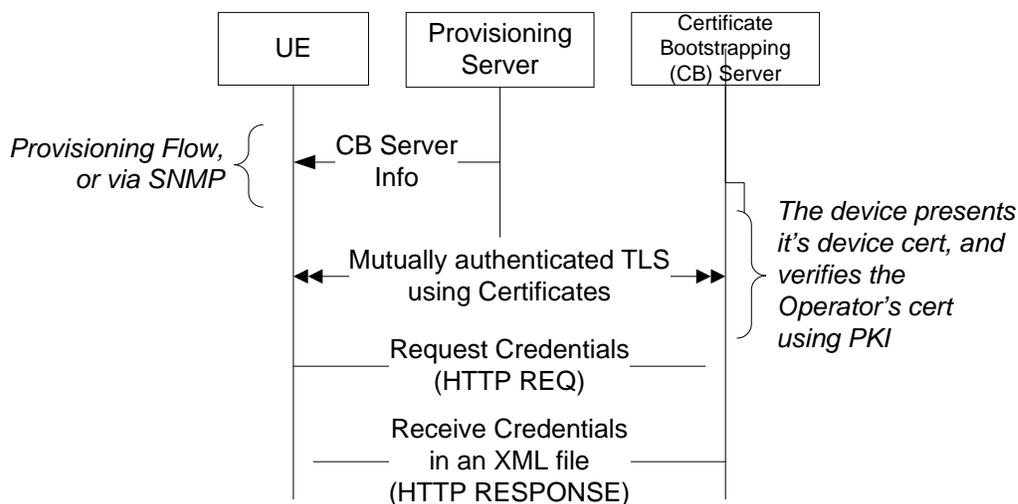

Figure 5 - Certificate Bootstrapping Flow (conceptual)

The following general requirements apply.

- The eUE MUST NOT use Certificate Bootstrapping unless triggered via a management interface (e.g., SNMP) or via configuration (e.g., configuration file). When triggered via the configuration file, the eUE MUST initiate the Certificate Bootstrapping procedure after the successful processing and acceptance of the configuration file parameters, i.e., after it generates the configuration processing events such as 'pass' or 'passWithWarnings'. Further, when the Certificate Bootstrapping is initiated via the configuration file, the eUE MUST initiate the Certificate Bootstrapping process prior to any SIP registrations, even if the eUE already contains IMPI entries in the MIB table 'pktcEUEUsrIMPITable'.

- The eUE SHOULD 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 [RFC 2246] and TLS_RSA_WITH_AES_128_CBC_SHA as described in [RFC 3268].

- 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 [RFC 2246] by validating a presented server certificate.

- The Certificate Bootstrapping Server MUST authenticate by the eUE as specified in [RFC 2246] 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.

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

6.7   E-UE Provisioning Interoperability

The major part of the requirements in this document are related to the mandatory support by the eUE of the dual-stack IP addressing. Contrasted with the previous versions of this document, where such support was not required, the dual-stack requirement introduces interoperability issues, which need to be considered when a mixture of the eUEs with various levels of compliancy are used in the field. This section considers such issues in accordance with the particular deployment scenarios possible in the field.

1. DSS capable eUEs deployed in the DSS aware Provisioning System

   - **Provisioning Plane:** In the case the eUE and Provisioning System are compliant with the requirements of this specification, there are no interoperability issues for the eUE provisioning. The eUE-s will be selecting its IP Addressing Mode as described in Table 8.

     To guarantee that the Provisioning System can recognize the "dual-stack capable" eUE-s, the Provisioning Server MUST consider the EUE to be the "dual-stack capable" (or the "new" one) if the eCM provides the IP_PREF DHCP Options (value b'111) in the DHCP message exchange.

   - **Signaling and Media Plane**: There are no interoperability issues on the Signaling and Media plane as well. P-CSCFs are provisioned as either IP addresses or FQDNs. FQDNs are resolved based on A and AAAA records. Normal selection of P-CSCF is performed per [PKT-EUE-DATA].

   - To guarantee that the PC 2.0 network has sufficient information on the ability of the eUE to support Dual-Stack capability, the eUE MUST include the new eUE Dual-Stack Support Capability as defined in Annex A.

2. DSS capable eUEs are deployed in a single stack network

   - **Provisioning Plane**: In case the eUE is compliant with this specification and deployed in a Provisioning System, which is not aware of DSS, there are no interoperability issues. The eCM DHCP options it (e.g., IP_PREF) and in the eUE Capability TLV (TLV 5.38) are ignored by the Provisioning Server. The eUE will select its IP Addressing Mode as described in the Table 8.

Table 8 - eUE IP Addressing Mode Selection for the Interoperability Case 2

When the eCM requests, via DHCPv4 DISCOVER or DHCPv6 ADVERTISE	And the eCM's DHCP Server Response (DHCPv4 ACK or DHCPv6 REPLY) contains	Then the eUE initialization and IP addressing mode is determined as follows
eUE DHCPv4 server addresses and DHCPv6 DSS IDs	- eUE IPv4-only address acquisition mode (IP_PREF = b'001); - Valid DHCPv4 server address(es)	IPv4, unless explicit indicator to shutdown the eUE see [PKT-PROV1.5].
	- eUE IPv6-only address acquisition mode (IP_PREF = b'010) - Valid DHCPv6; DSS ID(s)	IPv6, unless explicit indicator to shutdown the eUE (see Section 6.4.1).
	No Preference; contains valid eUE DHCPv4 server address(es)	IPv4, unless explicit indicator to shutdown the eUE [PKT-PROV1.5].

When the eCM requests, via DHCPv4 DISCOVER or DHCPv6 ADVERTISE	And the eCM's DHCP Server Response (DHCPv4 ACK or DHCPv6 REPLY) contains	Then the eUE initialization and IP addressing mode is determined as follows
	No preference; contains valid eUE DHCPv6 DSS ID(s) only	IPv6, unless explicit indicator to shutdown the eUE (see Section 6.4.1).
	Neither eUE DHCPv4 server address(es) nor eUE DHCPv6 server DSS_ID(s)	The eUE does not attempt to provision and remains dormant until it is reinitialized by the eCM.

- **Signaling and Media Plane**: If a DSS capable eUE is deployed in a PC2.0 network, which is single stack, then the Provisioning System is expected to provide the appropriate list of P-CSCF addresses or FQDNs to obtain IP connectivity and SIP registration.

3. Single stack eUE deployed in a DSS aware Provisioning System

- **Provisioning Plane**: In case the eUE is NOT compliant with this specification and is deployed in the Provisioning System DSS aware, then to guarantee that this deployment scenario can provide operational conditions the following requirements are applicable:

  o The Provisioning Server MUST consider the eUE to be the DSS non-capable if eCM DHCP message request does not contain IP_PREF DHCP Option.

  o The Provisioning Server MUST NOT provide values b'101' and b'110' in the IP_PREF DHCP Option for the "old" eUE.

  o eUE Provisioning Server MUST consider the eUE to be single stack (or the "old" eUE) if eUE capability string in DHCP message exchange does not contain the TLV 5.38 (as defined in Annex A).

- **Signaling and Media Plane**: There are no interoperability issues on the Signaling and Media plane as well. P-CSCFs are provisioned as either IP addresses or FQDNs. IP address resolution for the FQDNs is via DNS "A" and "AAAA" records. Normal selection of P-CSCF is performed per [PKT-EUE-DATA], and the eUE MUST register with the P-CSCF IP address of the same IP mode that is used to for the eUE's primary IP Address. Also, for communicating with the P-CSCF, the eUE MUST use the primary IP address.

Annex A   eUE Capabilities (Normative)

A.1   eUE Capabilities

An eUE MUST report all the following capabilities specified in [PKT-PROV1.5], in the section titled "MTA DEVICE CAPABILITIES", as well as any enhancements provided in Annex A.2.

- TLV 5.1 – PacketCable Version

- TLV 5.3 – TGT Support

- TLV 5.4 – HTTP Download File Access Method Support

It is to be noted that some of the non-required capabilities may be reused by PacketCable Application Specifications.

A.2   Capability Enhancements

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

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

This TLV indicates whether or not the eUE supports the Certificate Bootstrapping functionality. An eUE MUST include this TLV in the Capabilities String.

Type	Length	Values	Comment	Default Value
5.26	1	0	0: No	None
		1	1: Yes	

This TLV indicates whether or not the eUE has the capability to acquire both versions of IP addresses. An eUE MUST include this TLV in the Capabilities String with value 1.

Type	Length	Values	Comment	Default Value
5.38	1	0	0: Single Stack support	0
		1	1: Dual Stack Support	

Appendix I   Acknowledgements

CableLabs wishes to thank the PacketCable PACM focus team participants for various contributions and efforts that led to the development of this specification. Specifically:

- Eugene Nechamkin (Broadcom)

- Thomas Clack (Broadcom)

- John Berg (CableLabs)

- Sumanth Channabasappa (CableLabs)

- Josh Littlefield (Cisco)

- Donald Lukacs (Telcordia)

- Satish Kumar (Texas Instruments).

Special appreciation is extended to Eugene Nechamkin as the primary author, and for coordinating the various contributions through the development of this document. Appreciation is also extended to the following subject matter experts, contributors and reviewers: John Berg and Satish Kumar for provisioning flows and configuration file requirements, Josh Littlefield for IP configuration and IPv6 related requirements, Thomas Clack for data models and management requirements, and Don Lukacs for his numerous reviews and editorial feedback.

Eduardo Cardona and the PacketCable Architects, CableLabs, Inc.

Appendix II   Revision History

The following Engineering Change Notices were incorporated in PKT-SP-EUE-PROV-I02-080710.

ECN	ECN Date	Summary
EUE-PROV-N-08.0503-6	5/19/2008	Incorporation of feedback from the PacketCable 2.0 Provisioning and ATP Focus Teams
EUE-PROV-N-08.0505-8	5/27/2008	Incorporation of feedback from vendor and ATP focus teams

The following Engineering Change Notice was incorporated in PKT-SP-EUE-PROV-I03-090528.

ECN	ECN Date	Summary
EUE-PROV-N-09.0557-2	4/27/2009	Clarification to Battery Backup Requirements

The following Engineering Change Notice was incorporated in PKT-SP-EUE-PROV-I04-100120.

ECN	ECN Date	Summary
EUE-PROV-N-09.0604-2	11/23/2009	Clarifications on DHCPv6 OPTION_FQDN Requirements

The following Engineering Change Notices were incorporated in PKT-SP-EUE-PROV-I05-100527.

ECN	ECN Date	Summary
EUE-PROV-N-10.0632-2	5/3/2010	Clarifications Certificate Bootstrapping persistence
EUE-PROV-N-10.0634-1	4/26/2010	TFTP Block size fixing for IPV4 and IPV6

The following Engineering Change Notices were incorporated in PKT-SP-EUE-PROV-I06-110127.

ECN	ECN Date	Summary
EUE-PROV-N-10.0639-2	9/7/2010	eUE Correlation ID usage in DHCPv6 message
EUE-PROV-N-10.0640-2	9/7/2010	ToD Enforcements updates to ECN EUE-PROV-N-10.0642-1
EUE-PROV-N-10.0641-1	9/7/2010	Forcing eCM to retrieve ToD when DHCP options change
EUE-PROV-N-10.0642-1	9/7/2010	Selecting the SYSLOG Server address when more than one SYSLOG server is configured in DHCPv6 option.
EUE-PROV-N-10.0645-3	12/20/2010	EUE Option 43.8 encoding
EUE-PROV-N-10.0647-3	12/20/2010	DHCP OPTION_VENDOR_OPTS (17) in ORO(6)

The following Engineering Change Notice was incorporated in PKT-SP-EUE-PROV-I07-110825.

ECN	ECN Date	Summary
EUE-PROV-N-11.0662-7	7/11/2011	EUE Dual IP Stack - New Features