

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.167

(12/2007)

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

IPCablecom

Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems

ITU-T Recommendation J.167



International
Telecommunication
Union
Documents

Document Sharing Hub

ITU-T Recommendation J.167

Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems

Summary

ITU-T Recommendation J.167 describes the IPCablecom media terminal adapter (MTA) device initialization and provisioning process. It is limited to the provisioning of an IPCablecom embedded-MTA device by a single provisioning and network management provider.

Source

ITU-T Recommendation J.167 was approved on 14 December 2007 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2008

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

CONTENTS

Page

1	Scope	1
2	References.....	1
2.1	Normative references.....	1
2.2	Informative references.....	2
3	Terms and definitions	3
4	Abbreviations and conventions.....	3
4.1	Abbreviations	3
4.2	Conventions.....	3
5	Introduction	4
5.1	Service goals.....	4
5.2	Specification goals.....	4
5.3	IPCablecom reference architecture.....	5
5.4	Components and interfaces.....	6
6	Provisioning overview	10
6.1	Device provisioning.....	10
6.2	Endpoint provisioning	10
6.3	Provisioning state transitions.....	10
6.4	Basic and hybrid flow provisioning state transitions	11
7	Provisioning flows.....	11
7.1	Backoff, retries and time-outs	12
7.2	Embedded-MTA power-on initialization flows	13
7.3	Embedded-MTA power-on initialization flow (Basic flow).....	24
7.4	Embedded-MTA power-on initialization flow (Hybrid flow).....	25
7.5	Endpoint provisioning completion notifications	28
7.6	Post initialization incremental provisioning.....	29
7.7	Reflecting the State of the endpoint interface in the ifTable.....	32
7.8	Provisioning of the signalling communication path between the MTA and CMS.....	33
7.9	MTA replacement.....	33
7.10	Temporary signal loss.....	33
7.11	MTA hard reboot/soft reset scenarios	33
8	DHCP options.....	33
8.1	DHCP option 122: Client configuration option.....	33
8.2	DHCP option 60: Vendor-client identifier	38
8.3	DHCP options 12 and 15	38
8.4	DHCP option 6	38
8.5	DHCP option 43	38
8.6	DHCP option 1	41

		Page
	8.7 DHCP option 3	41
	8.8 DHCP OPTION CL_V4_PACKETCABLE_MIB_ENV_OPTION.....	41
9	MTA provisionable attributes.....	42
	9.1 MTA configuration file	42
10	MTA device capabilities.....	56
	10.1 IPCablecom version.....	57
	10.2 Number of telephony endpoints	57
	10.3 TGT support	57
	10.4 HTTP download file access method support.....	57
	10.5 MTA24 event SYSLOG notification support.....	57
	10.6 NCS service flow support.....	58
	10.7 Primary line support	58
	10.8 Vendor specific TLV Type(s)	58
	10.9 NVRAM ticket/Ticket information storage support.....	58
	10.10 Provisioning event reporting support	58
	10.11 Supported CODEC(s).....	58
	10.12 Silence suppression support	59
	10.13 Echo cancellation support.....	59
	10.14 RSVP support	59
	10.15 UGS-AD support.....	59
	10.16 MTA's "ifIndex" starting number in "ifTable"	60
	10.17 Provisioning flow logging support.....	60
	10.18 Supported provisioning flows.....	60
	10.19 T38 version support.....	61
	10.20 T38 error correction support.....	61
	10.21 RFC 2833 DTMF support	61
	10.22 Voice metrics support.....	61
	10.23 Device MIB support	61
	10.24 Multiple grants per interval support	63
	10.25 V.152 Support.....	63
11	TLV-38 SNMP notification receiver specification.....	64
	11.1 Sub-TLVs of TLV-38.....	64
	11.2 Mapping of TLV fields into SNMP tables	66
	11.3 TLV-38 and TLV-11 configuration example.....	72
12	SNMPv2c management requirements	76
	12.1 SNMPV2c coexistence mode tables content created by MTA after MTA4 for hybrid and basic flows	77
	12.2 SNMP default entries for SNMPv2 access.....	78

	Page
13 Service interruption impact reporting and other enhanced features support	80
13.1 eDocsis requirements support.....	80
13.2 IPCablecom extension MIB	81
13.3 Battery backup MIBs.....	81
13.4 Syslog MIBs	81
13.5 Foreign potential detection	81
Appendix I – SNMPv2c coexistence configuration example – Template for service providers	82

.....

Copyright International Telecommunication Union/ITU Telecommunication Sector

ITU-T Recommendation J.167

Media terminal adapter (MTA) device provisioning requirements for the delivery of real-time services over cable television networks using cable modems

1 Scope

This Recommendation describes the IP-Cablecom media terminal adapter (MTA) device initialization and provisioning process. It is limited to the provisioning of an IP-Cablecom embedded-MTA device by a single provisioning and network management provider.

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

2 References

2.1 Normative references

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

- [ITU-T J.83] ITU-T Recommendation J.83 (2007), *Digital multi-programme systems for television, sound and data services for cable distribution*.
- [ITU-T J.112.B] ITU-T Recommendation J.112 Annex B (2004), *Data-over-cable service interface specifications: Radio-frequency interface specification*.
- [ITU-T J.162] ITU-T Recommendation J.162 (2007), *Network call signalling protocol for the delivery of time-critical services over cable television networks using cable modems*.
- [ITU-T J.166] ITU-T Recommendation J.166 (2007), *IP-Cablecom Management Information Base (MIB) framework*.
- [ITU-T J.170] ITU-T Recommendation J.170 (2005), *IP-Cablecom security specification*.
- [IETF RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.
- [IETF RFC 2132] IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*.
- [IETF RFC 2475] IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.
- [IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*.
- [IETF RFC 2833] IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.
- [IETF RFC 2863] IETF RFC 2863 (2000), *The Interfaces Group MIB*.
- [IETF RFC 3396] IETF RFC 3396 (2002), *Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)*.

- [IETF RFC 3410] IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework*.
- [IETF RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.
- [IETF RFC 3412] IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*.
- [IETF RFC 3413] IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.
- [IETF RFC 3414] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.
- [IETF RFC 3415] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.
- [IETF RFC 3495] IETF RFC 3495 (2003), *Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration*.
- [IETF RFC 3584] IETF RFC 3584 (2003), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.
- [IETF RFC 3594] IETF RFC 3594 (2003), *PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option*.
- [IETF RFC 3617] IETF RFC 3617 (2003), *Uniform Resource Identifier (URI) Scheme and Applicability Statement for the Trivial File Transfer Protocol (TFTP)*.

2.2 Informative references

- [IETF RFC 3315] IETF RFC 3315 (2003), *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*.
- [IETF RFC 4682] IETF RFC 4682 (2006), *Multimedia Terminal Adapter (MTA) Management Information Base for PacketCable- and IPCompliant Devices*.
- [IETF RFC 5098] IETF RFC 5098 (2008), *Signaling MIB for PacketCable and IPCompliant Multimedia Terminal Adapters (MTAs)*.
- [IETF-draft-eventmess] IETF Internet Draft, *Management Event Management Information Base (MIB) for PacketCable- and IPCompliant Devices*, October 2006, <http://www.ietf.org/internet-drafts/draft-ietf-ipcdn-pktn-eventmess-09.txt>, work in progress.
- [DOCSIS 3.0] Data-Over-Cable Service Interface Specifications, *DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*, CM-SP-MULPIv3.0-I02-061222, June 12, 2006, Cable Television Laboratories, Inc.
- [ITU-T J.222.2] ITU-T Recommendation J.222.2 (2007), *Third-generation transmission systems for interactive cable television services – IP cable modems: MAC and upper layer protocols*.
- [CableLabs' DHCP] *CableLabs' DHCP Options Registry Specification*, CL-SP-CANN-DHCP-Reg-I01-070119, January 19, 2007, Cable Television Laboratories, Inc.

3 Terms and definitions

This Recommendation defines the following terms:

3.1 cable modem: A cable modem is a layer-two termination device that terminates the customer end of the J.112 connection.

3.2 IPCablecom: An ITU-T project that includes an architecture and a series of Recommendations that enable the delivery of real-time services (such as telephony) over the cable television networks using cable modems.

4 Abbreviations and conventions

4.1 Abbreviations

This Recommendation uses the following abbreviations:

CM	Cable Modem
CMS	Call Management Server
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
MAC	Media Access Control
MTA	Media Terminal Adapter
PSTN	Public Switched Telephone Network
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
TGS	Ticket Granting Server

4.2 Conventions

It is understood that implementing this Recommendation is optional. If this Recommendation is implemented, the key words "MUST" and "SHALL" as well as "REQUIRED" are to be interpreted as indicating a mandatory aspect of this Recommendation. The key words indicating a certain level of significance of particular requirements that are used throughout this Recommendation are summarized below:

"MUST"	This word or the adjective "REQUIRED" means that the item is an absolute requirement of this Recommendation.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this Recommendation.
"SHOULD"	This word or the adjective "RECOMMENDED" means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.

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

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

5 Introduction

5.1 Service goals

Cable operators are interested in deploying high-speed data communications systems on cable television networks. The intended service enables voice communications, video and data services based on bidirectional transfer of Internet Protocol (IP) traffic, between the cable system headend and customer locations, over an all-coaxial or hybrid-fibre/coax (HFC) cable network, defined by DOCSIS Recommendations. This is shown in simplified form in Figure 1.

NOTE – The term "DOCSIS" in this Recommendation is understood to refer to DOCSIS version 1.1 (ITU-T Rec. J.112), DOCSIS 2.0 (ITU-T Rec. J.122) or DOCSIS 3.0 (ITU-T Recs J.222.x), unless explicitly specified otherwise. Implementations of eCMs will refer to the corresponding DOCSIS versions and associated requirements in this Recommendation and DOCSIS Recommendations for compliance.

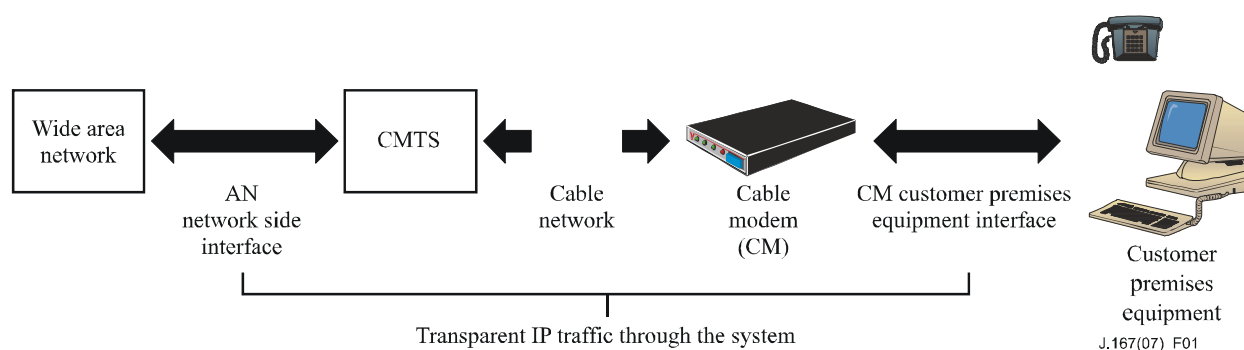


Figure 1 – Transparent IP traffic through the data-over-cable system

The transmission path over the cable system is realized at the headend by a cable modem termination system (CMTS), and at each customer location by a cable modem (CM). The intent is for operators to transfer IP traffic transparently between these interfaces.

5.2 Specification goals

Requirements relevant to device provisioning are:

- A single physical device (e.g., embedded-MTA) will be completely provisioned and managed by a single business entity. This provider may establish business relationships with additional providers for services such as data, voice communications and other services.
- To provision an E-MTA, both the DOCSIS and IPCablecom provisioning steps MUST be performed. The eMTA MUST have its own IP address, different from the IP Address(es) of the eCM. The eMTA MUST also have its own MAC address, different from the MAC address of the eCM. Furthermore, the E-MTA MUST be able to operate in environments where the eMTA IP address may be in the same, or different subnet as the eCM.

- IPCom requires a unique FQDN for the MTA-component in the embedded-MTA. This FQDN MUST be included in the DHCP OFFER and DHCP ACK messages to the MTA-component. IPCom makes no additional FQDN requirements on the CM component in the embedded-MTA beyond those required by DOCSIS. Mapping of the FQDN to IP address MUST be configured in the network DNS server and be available to the rest of the network.
- IPCom embedded-MTA provisioning MUST use DHCP Option 12 and Option 15 to deliver the MTA FQDN to the E-MTA.
- IPCom embedded-MTA provisioning MUST support two separate configuration files: J.112-specified configuration file for the CM component, and an IPCom-specified configuration file for the MTA component.
- The embedded-MTA is outside the IPCom network trust boundary as defined in the IPCom architecture J.160.
- IPCom E-MTA MUST support DOCSIS software download as defined in the corresponding eCM DOCSIS Recommendation. A single DOCSIS software download MUST be used to upgrade code for both the eCM and the eMTA.
- IPCom MUST support use of SNMPv2c coexistence for network management operations for devices provisioned under the Basic Flow or the Hybrid Flow and SNMPv3/v2 coexistence for network management operations when the device is provisioned under the Secure Flow.
- IPCom embedded-MTA provisioning minimizes the impact to DOCSIS devices (CM and CMTS) in the network.
- Standard server solutions (TFTP, SNMP, DNS, etc.) are preferable. It is understood that an application layer may be required on top of these protocols to coordinate IPCom embedded-MTA provisioning.
- Where appropriate, the DOCSIS management protocols are supported (e.g., SNMP).

5.3 IPCom reference architecture

Figure 2 shows the reference architecture for the IPCom Network. Refer to the IPCom architecture J.160 for more detailed information on this reference architecture.

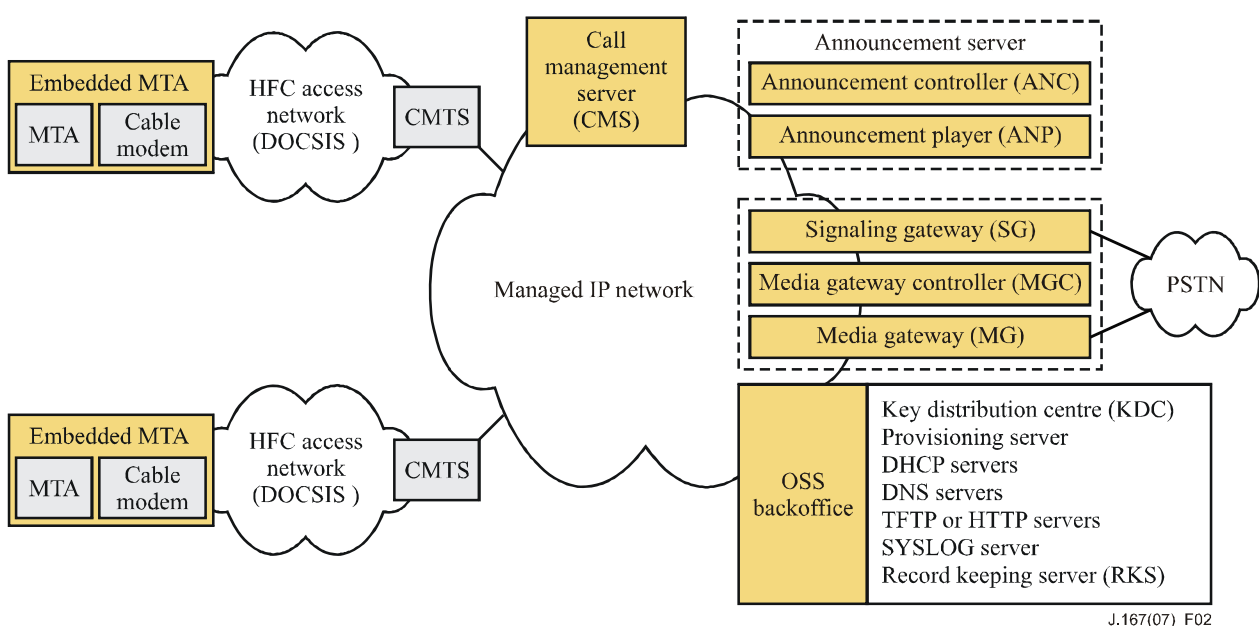


Figure 2 – IPCom network component reference model (partial)

5.4 Components and interfaces

The basic IP-Cablecom embedded-MTA provisioning reference architecture is shown in Figure 3. This figure represents the components and interfaces discussed in this Recommendation.

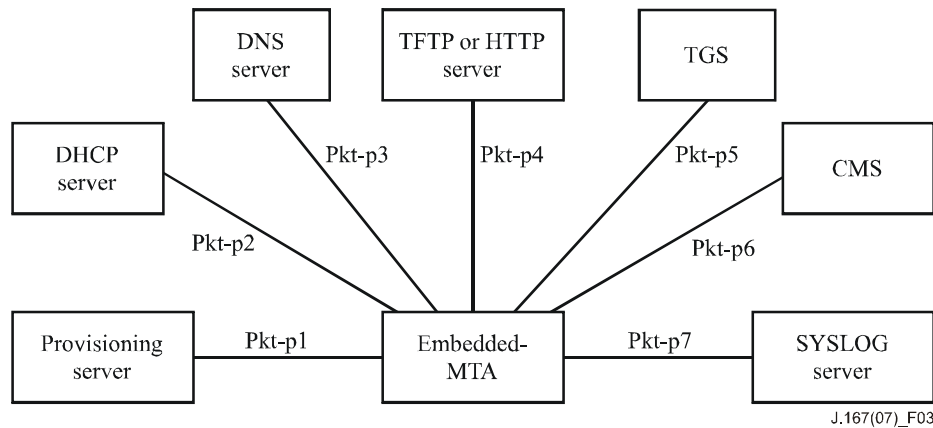


Figure 3 – IP-Cablecom provisioning interfaces

5.4.1 MTA

The MTA MUST conform to the following requirements during the provisioning sequence.

5.4.1.1 MTA security requirements

The MTA MUST conform to the following security requirements during the Secure Flow provisioning sequence:

- The MTA device MIB is structured to represent the assignment of MTA endpoints to a CMS. For more information on the security association between an MTA and a CMS, refer to [ITU-T J.170].
- CMS Kerberos Principal Name is not explicitly configured in the MTA endpoints. The MTA MUST be able to determine the CMS Kerberos Principal Name based on the CMS FQDN, as specified in [ITU-T J.170].
- For each unique pair of CMS Kerberos principal Name/Kerberos Realm assigned to an endpoint, the MTA MUST obtain a single Kerberos ticket per [ITU-T J.170].
- If the MTA already has a valid Kerberos ticket for that CMS, the MTA MUST NOT request an additional Kerberos ticket for that CMS. (Unless the expiration time of the current Kerberos ticket $\leq$ current time + PKINIT Grace Period, in which case the MTA MUST obtain a fresh ticket for the same CMS.)
- In the case that a CMS FQDN maps to multiple IP addresses, the MTA MUST initially establish a pair of IPsec Security Associations with one of the IP addresses returned by the DNS server. The MTA MAY also initially establish IPsec Security Associations with the additional CMS IP addresses. See [ITU-T J.170] for more information.
- If the MTA already has a pair of active Security Associations (inbound and outbound) with a particular CMS IP address, the MTA MUST NOT attempt to establish additional Security Associations with the same IP address.

During the provisioning sequence, there are no specific security requirements for the Basic Flow or the Hybrid Flow.

5.4.1.2 MTA SNMP requirements

The MTA MUST conform to the following SNMPv3 requirements during the Secure Flow provisioning sequence:

- MTA SNMPv3 security is separate and distinct from CM SNMPv3 security. USM security information (authentication and privacy keys, and other USM table entries) is set up separately.
- SNMPv3 initialization MUST be completed prior to the provisioning enrolment inform.
- In Secure Flow, the MTA MUST support SNMPv3 and SNMPv2 based device management as defined in [IETF RFC 3414] and [IETF RFC 3584].

The MTA MUST conform to the following SNMPv2c requirements during the Hybrid Flow or Basic Flow provisioning sequence:

- SNMPv2c initialization MUST be completed immediately after the DHCP phase.
- SNMPv2c based device management is defined in [IETF RFC 3584].

The MTA MUST implement the management information base (MIB) modules as described in IETF RFC 1945 and specified in Annexes B, D, E and F of [ITU-T J.166]. If it also implements the IETF MIB modules as specified in [IETF RFC 4682], [IETF RFC 5098] and [IETF-draft-eventmess], the MTA MUST ensure that both sets of MIB modules can coexist without any conflicting or ambiguous behaviour. MTAs implementing multiple MIB environments MUST support the DHCP option 'CL_V4_PACKETCABLE_MIB_ENV_OPTION' as specified in clauses 7 and 8.8.

It is understood that any MIB module or MIB Object references in this Recommendation refer to either MIB modules unless explicitly specified otherwise, or the MIB Object is specified in only one of them.

5.4.2 Provisioning server

The Provisioning Server is made up of the following components:

- Provisioning Application – The Provisioning Application is responsible for coordinating the embedded-MTA provisioning process. This application has an associated SNMP Entity.
- Provisioning SNMP Entity – The provisioning SNMP entity MUST include a trap/inform handler for provisioning enrolment and the provisioning status traps/informs as well as an SNMP engine for retrieving device capabilities and setting the Configuration filename and access method. Refer to the IPCablecom MTA MIB [ITU-T J.166] or [IETF RFC 4682] for a description of the MIB accessible MTA attributes.
- The Provisioning Server MUST examine the "Device MIB Support" capability of the MTA (specified in clause 10.23) to choose the MIB modules that can be used to specify the MTA configuration file.

The interface between the Provisioning Application and the associated SNMP Entity is not specified in IPCablecom and is left to vendor implementation. The interface between the Provisioning Server and the TFTP Server is not specified in IPCablecom and is left to vendor implementation.

5.4.3 MTA to telephony Syslog server

The IPCablecom MTAs MUST implement Management Event Mechanism as per ITU-T Rec. J.172, which includes the support for Syslog server.

The IPCablecom MTAs MUST also implement all the IPCablecom Provisioning Management Events described in Annex A/J.172.

5.4.4 MTA to DHCP server

This interface identifies specific requirements in the DHCP server and the client for IP assignment during the MTA initialization process:

- Both the DHCP server and the embedded-MTA MUST support DHCP option codes 6, 7, 12, 15, 43, 60 and DHCP option code 122 (defined in [IETF RFC 2132]). Option codes 12 (Host Name) and 15 (Domain Name) MUST form a Fully Qualified Domain Name and MUST be resolvable by the DNS server.
- The DHCP server MUST accept and support broadcast and unicast messages per [IETF RFC 3396] from the MTA DHCP client.
- The DHCP server MUST include the MTA's assigned FQDN in the DHCP OFFER and DHCP ACK messages to the MTA-component of the embedded-MTA. Refer to [IETF RFC 2131] for details describing the DHCP OFFER message.

5.4.5 MTA to provisioning application

This interface identifies specific requirements for the Provisioning Application to satisfy MTA initialization and registration. The Provisioning Application requirements are:

- The MTA MUST generate a correlation ID – An arbitrary value that will be exchanged as part of the device capability data to the Provisioning Application. This value is used as an identifier to correlate related events in the MTA provisioning sequence.
- The Provisioning Application MUST provide the MTA with its MTA configuration data file. The MTA configuration file is specific to the MTA-component of the embedded-MTA and separate from the CM-component's configuration data file.
- The configuration data file format is TLV binary data suitable for transport over the specified TFTP or HTTP access method.
- The Provisioning Application MUST have the capability to configure the MTA with different data and voice service providers.
- The Provisioning Application MUST use only SNMPv3 to provision devices in the Secure Flow. The support of the Basic and Hybrid Flows is optional for the Provisioning Application. If the Basic and Hybrid Flows are supported, the Provisioning Application MUST use only SNMPv2c to provision devices in the Hybrid or Basic Flow.
- The Provisioning Application MUST provide SNMPv3 and SNMPv2 for device management.
- The Provisioning Application MUST support online incremental device/subscriber provisioning using SNMP.
- MTA MUST Specify all of its Capabilities in DHCP option 60 in accordance with clause 10.
- Provisioning Application MUST NOT assume any Capabilities, which do not have default values. In case capabilities supplied by the MTA are not consistent in format and/or in number and/or in values, the Provisioning Application MUST use the other means to identify the MTA's capabilities (e.g., SNMPv3 if possible).

5.4.6 MTA to CMS

Signalling is the main interface between the MTA and the CMS. Refer to the IPCablecom signalling [ITU-T J.162] for a detailed description of the interface.

- The CMS MUST accept signalling and bearer channel requests from an MTA that has an active security association.

- The CMS MUST NOT accept signalling and bearer channel requests from an MTA that does not have an active security association unless provisioned to do so with information corresponding to the "pktnMtaDevCmsIpsecCtrl" MIB Object.

5.4.7 MTA to security server (KDC)

The interface between the MTA and the key distribution centre (KDC) MUST conform to the [ITU-T J.170] IPsec security specification.

AP-REQ/REP exchange backoff and retry mechanism of the Kerberized SNMPv3 key negotiation defined in [ITU-T J.170] is controlled by the values delivered by DHCP option 122 sub-option 5 (see clause 8.1.4).

AS-REQ/REP exchange backoff and retry mechanism of the Kerberized SNMPv3 key negotiation defined in [ITU-T J.170] is controlled by the values delivered by DHCP option 122 sub-option 4 (see clause 8.1.3) or by the default values of the corresponding MIB objects in the Realm Table if sub-option 4 is not present in the DHCP option 122.

5.4.8 MTA and configuration data file access

This Recommendation allows for more than one access method to download the configuration data file to the MTA:

- The MTA MUST support the TFTP access method for downloading the MTA configuration data file.
- The MTA MAY support HTTP access method for downloading the MTA configuration data file.
- The Provisioning Server MUST provide the MTA with the URL-encoded TFTP/HTTP server address and configuration filename via a SNMPv3 SET for the Secure Flow. The Provisioning Server MUST provide the MTA with the URL-encoded TFTP/HTTP server address via an SNMPv2c SET if it supports the Hybrid Flow provisioning mode. The Basic Flow does not require an SNMP SET to get the configuration file; the Provisioning Server MUST provide the MTA with the TFTP/HTTP server address in the DHCP "file" and "siaddr" fields if it supports the Basic Flow provisioning mode. For additional information, refer to clause 7.3.

5.4.9 DOCSIS extensions for MTA provisioning

This Recommendation requires that the following additions to DOCSIS flows for MTA auto-provisioning be supported:

- eCMs that can obtain IP configuration information from multiple DHCP servers MUST use the primary DHCP server – designated to provide the eCM configuration information – for obtaining IPsec specific options (refer to [ITU-T J.222.2] for more information).
- eCMs relying on DHCPv4 for IPsec specific information MUST implement DHCP option code 122 (as specified in IETF RFC 3442) and communicate the Telephony Service Provider's DHCPv4 Server information to the eMTA (as per clause 7).
- eCMs relying on DHCPv6 for IPsec specific information MUST implement the DHCP option code OPTION_VENDOR_OPTS(17) (as specified in [IETF RFC 3315]) and the "CableLabs Client Configuration" DHCPv6 option code CL_OPTION_CCC (as specified in Annex A of [ITU-T J.166]) to communicate the Telephony Service Provider's DHCPv4 Server information to the eMTA.

6 Provisioning overview

Provisioning is a subset of configuration management control. The provisioning aspects include, but are not limited to, defining configurable data attributes, managing defined attribute values, resource initialization and registration, managing resource software, and configuration data reporting. The resource (also referred to as the managed resource) always refers to the MTA device. Further, the associated subscriber is also referred to as a managed resource.

6.1 Device provisioning

Device provisioning is the process by which an embedded-MTA device is configured to support voice communications service.

Device provisioning involves the MTA obtaining its IP configuration required for basic network connectivity, announcing itself to the network and downloading of its configuration data from its provisioning server.

When the device is provisioned using the "Secure Flow", the MTA device **MUST** be able to verify the authenticity of the configuration file it downloads from the server. The "Secure Flow" generated configuration file is "signed" and may be "sealed". Refer to [ITU-T J.170] for further information.

Refer to clause 5.4.1 for provisioning rules related to security associations.

When the device is provisioned using the Basic Flow or the Hybrid Flow, a content integrity verification check **MUST** be conducted on the configuration file by the MTA. For details, refer to clause 9.1.

6.2 Endpoint provisioning

Endpoint provisioning is when a provisioned MTA authenticates itself to the CMS and establishes a security association with that server. This allows subsequent call signalling to be protected under the established security association.

The MTA **MUST** follow the requirements defined in the IPCablecom security specification [ITU-T J.170] for NCS Kerberized Key Management, independently of the provisioning flow (Secure, Hybrid or Basic Flow) the MTA was provisioned with.

6.3 Provisioning state transitions

Figure 4 represents logical device states and the possible transitions across these logical states. This representation is for illustrative purposes only and is not meant to imply a specific implementation. The following MTA state transitions do not specify the number of retry attempts or retry time out values:

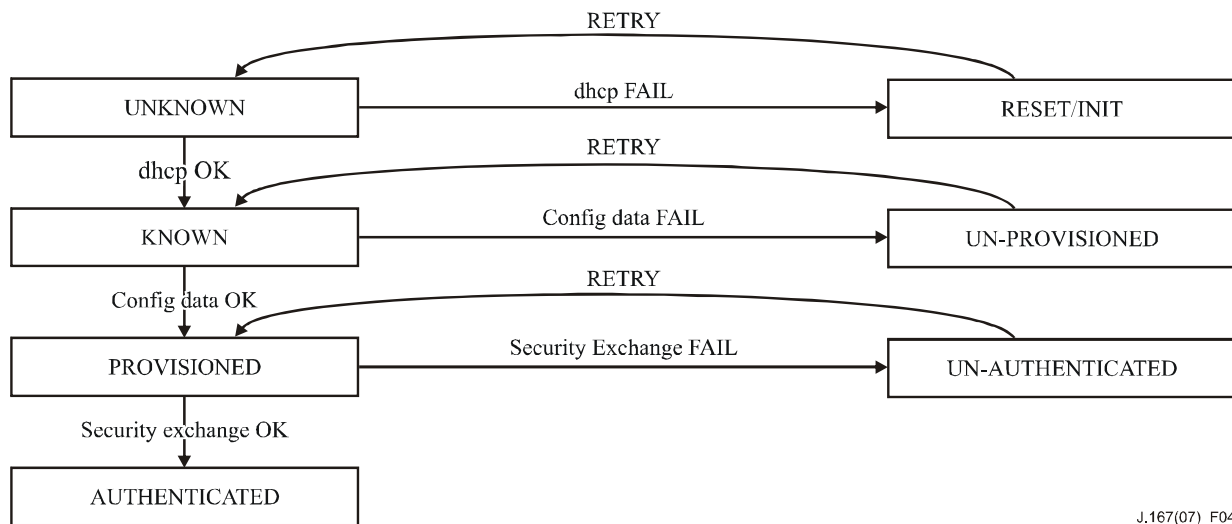


Figure 4 – Device states and state transitions for secure flow provisioning

6.4 Basic and hybrid flow provisioning state transitions

Figure 5 represents logical device states and the possible transitions across these logical states. This representation is for illustrative purposes only and is not meant to imply a specific implementation. The following MTA state transitions do not specify the number of retry attempts or retry time out values.

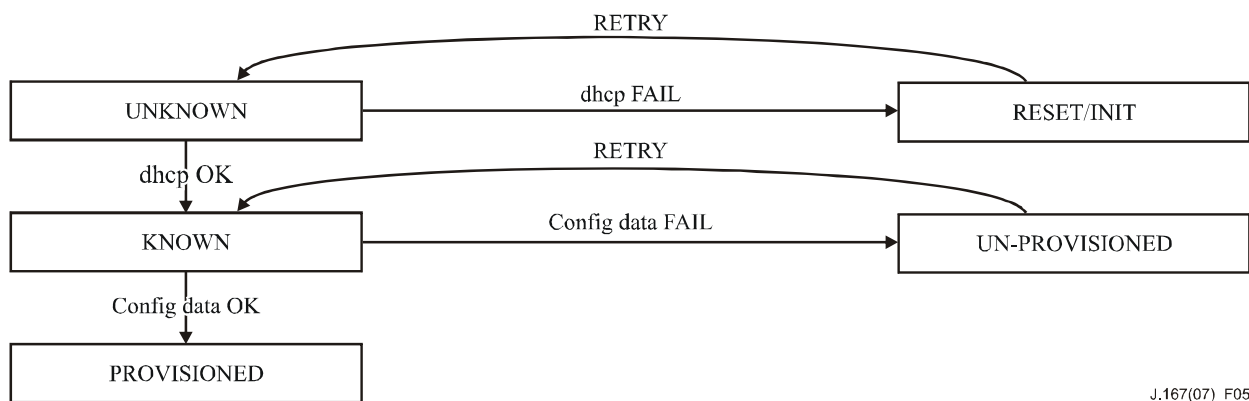


Figure 5 – Device states and state transitions for basic and hybrid flow provisioning

7 Provisioning flows

An IPCablecom MTA is provisioned via one of three provisioning flows:

- The Secure Flow supports Kerberos mutual authentication between the MTA and the provisioning system, as well as Kerberized SNMPv3 messaging. The Secure Flow **MUST** be supported by IPCablecom MTAs and the Provisioning Applications.
- The Basic Flows are a simplified DOCSIS-like provisioning flows with no Kerberos or SNMPv3 security and no SNMP enrolment via SNMP INFORM. The Basic Flows **SHOULD** be supported by IPCablecom MTAs and Provisioning Applications.
- The Hybrid Flows are essentially the Secure flow with the Kerberos message exchanges removed, and SNMPv2c substituted for SNMPv3. The Hybrid Flows **SHOULD** be supported by IPCablecom MTAs and Provisioning Applications.

Any mention of SNMP in this Recommendation without a specific reference to the SNMP protocol version must be interpreted as follows:

- For the Secure Flow, the MTA MUST support 'SNMPv3 only' for Provisioning and SNMPv3/v2c coexistence for Network Management and/or Monitoring operations. The SNMPv3/v2c coexistence MUST be supported and is configured using the values of TLV-38, or TLV-11 and TLV-64 in the MTA configuration file.
- For the Hybrid or Basic Flows, the MTA MUST support SNMPv2c for Provisioning, Network Management and/or Monitoring operations. The level of SNMPv2c access MUST be supported according to the values of TLV-38 or TLV-11 and TLV-64 in the MTA configuration file.

An MTA can also be configured with additional SNMPv2c targets via its configuration file by using TLV-38 or TLV-11 and TLV-64.

An MTA is commanded to execute a specific flow via the contents of DHCP option 122 sub-option 6, as described in clause 8.1.5. Each of these flows begins with a common set of flow steps.

An MTA is required to implement the IPCablecom specified MIBs, and optionally may implement the IETF MIBs. For an MTA supporting both, the operator may wish to provide a preference for usage. An MTA that supports multiple MIB environments MUST request an appropriate DHCPv4 option. The DHCPv4 option "CL_V4_PACKETCABLE_MIB_ENV_OPTION (4)", as specified in the CableLabs' DHCP Options Registry could be used. The Provisioning Server MAY indicate an operator preference by responding with the DHCPv4 option "CL_V4_PACKETCABLE_MIB_ENV_OPTION (4)". The MTA requirements associated with this option are specified in clause 8.8.

In all the provisioning flows indicated in this clause, the following requirements apply:

- if an MTA encounters DHCP options that it does not recognize – in the DHCP OFFER or DHCP ACK messages – it MUST ignore such options and proceed with provisioning as though they were not provided (i.e., MTA operation is unaffected);
- if an IPCablecom Provisioning Server receives SNMP INFORMs from MTAs that contain Object Identifiers that it does not recognize, it SHOULD acknowledge them. Further, upon receiving any SNMP notifications containing unrecognized Object Identifiers, the Provisioning Server MUST comply with the behaviour specified in this Recommendation (i.e., Provisioning Server operation is unaffected).

7.1 Backoff, retries and time-outs

Backoff mechanisms help the network to throttle device registration during a typical or mass registration condition when the MTA client requests are not serviced within the protocol-specified time-out values. The details of provisioning behaviour under mass-registration is beyond the scope of IPCablecom; however, this clause provides the following recommendations and requirements:

- Throttling of registrations MAY be based on DOCSIS CM registration.
- The MTA MUST follow DHCP [IETF RFC 2131] and HTTP specification time-out and retry mechanisms. It is recommended to follow [IETF RFC 3413] for SNMP timeout and retry mechanisms.
- The MTA MUST use an adaptive time-out for TFTP as specified in DOCSIS (ITU-T Rec. J.112/J.122).

- The MTA MUST follow backoff and retry recommendations that are defined in [ITU-T J.170] security specification for the security message flows.
- All Provisioning Flows (Secure, Basic and Hybrid) are described in clauses 7.2, 7.3 and 7.4.
 - Provisioning timer MUST start immediately after the receipt of DHCP ACK and MUST end with the completion of TFTP/HTTP configuration file response.
 - In case the provisioning timer expires before the completion of TFTP/HTTP configuration file response, the MTA MUST return to MTA1.
 - MTA MUST NOT wait until the Provisioning Timer expires before acting on each Provisioning step's failure condition. For example, in Secure Flow, if step MTA19 fails, the MTA must not wait until the Provisioning Timer expires but must return to MTA1 immediately when the failure condition is discovered.
- In the Secure Provisioning Flow – If a failure occurs in any of the steps related to the PROV_SNMP_ENTITY (MTA13, MTA14, MTA15, MTA19) before the MTA obtains the Device configuration file – and the MTA resolved multiple IP addresses for the PROV_SNMP_ENTITY (FQDN received in option 122 sub-option 3), then it MUST retry the steps with all the resolved IP addresses before returning to MTA1, unless directed otherwise by [ITU-T J.170]. However, it is to be noted that once the MTA selects a resolved IP address for use in MTA13, it MUST use the same IP address in steps MTA15 and MTA25.
- In the Hybrid Provisioning Flow – If a failure occurs in any of the steps related to the PROV_SNMP_ENTITY (H-MTA15, H-MTA19) before the MTA obtains the Device configuration file – and the MTA resolved multiple IP addresses for the PROV_SNMP_ENTITY (FQDN received in option 122 sub-option 3), then it MUST retry the steps with all the resolved IP addresses before returning to MTA1. However, it is to be noted that once the MTA selects a resolved IP address for use in H-MTA15, it MUST use the same IP address in H-MTA25.

7.2 Embedded-MTA power-on initialization flows

Table 1 shows the mandatory message flow that the embedded-MTA device MUST follow during power-on initialization (unless stated explicitly otherwise). It is understood that these flows do not imply implementation or limit functionality.

Although these flows show the MTA configuration file download from a TFTP Server, the descriptive text details the requirements to support the MTA configuration file download from an HTTP Server.

Note in the flow details below that certain steps may appear to be a loop in the event of a failure. In other words, the step to proceed to if a given step fails is to retry that step again. However, it is recommended that if the desired number of backoff and retry attempts does not allow the step to successfully complete, the device detecting the failure should generate a failure event notification.

In the flow details below (see Figure 6 and Table 1), the calculation of the Hash and the Encryption/Decryption of the MTA's Configuration File MUST follow the requirements in [ITU-T J.170].

The provisioning flow for an eCM utilizing DHCPv4 for IP configuration is shown on Figure 6 and explained in clause 7.2.1. The provisioning flow for an eCM utilizing DHCPv6 for IP configuration is shown on Figure 6a and explained in clause 7.2.2. The provisioning flows for an eMTA remain the same, irrespective of the eCM provisioning mode.

7.2.1 Embedded-MTA secure power-on initialization flow (IPv4 eCM)

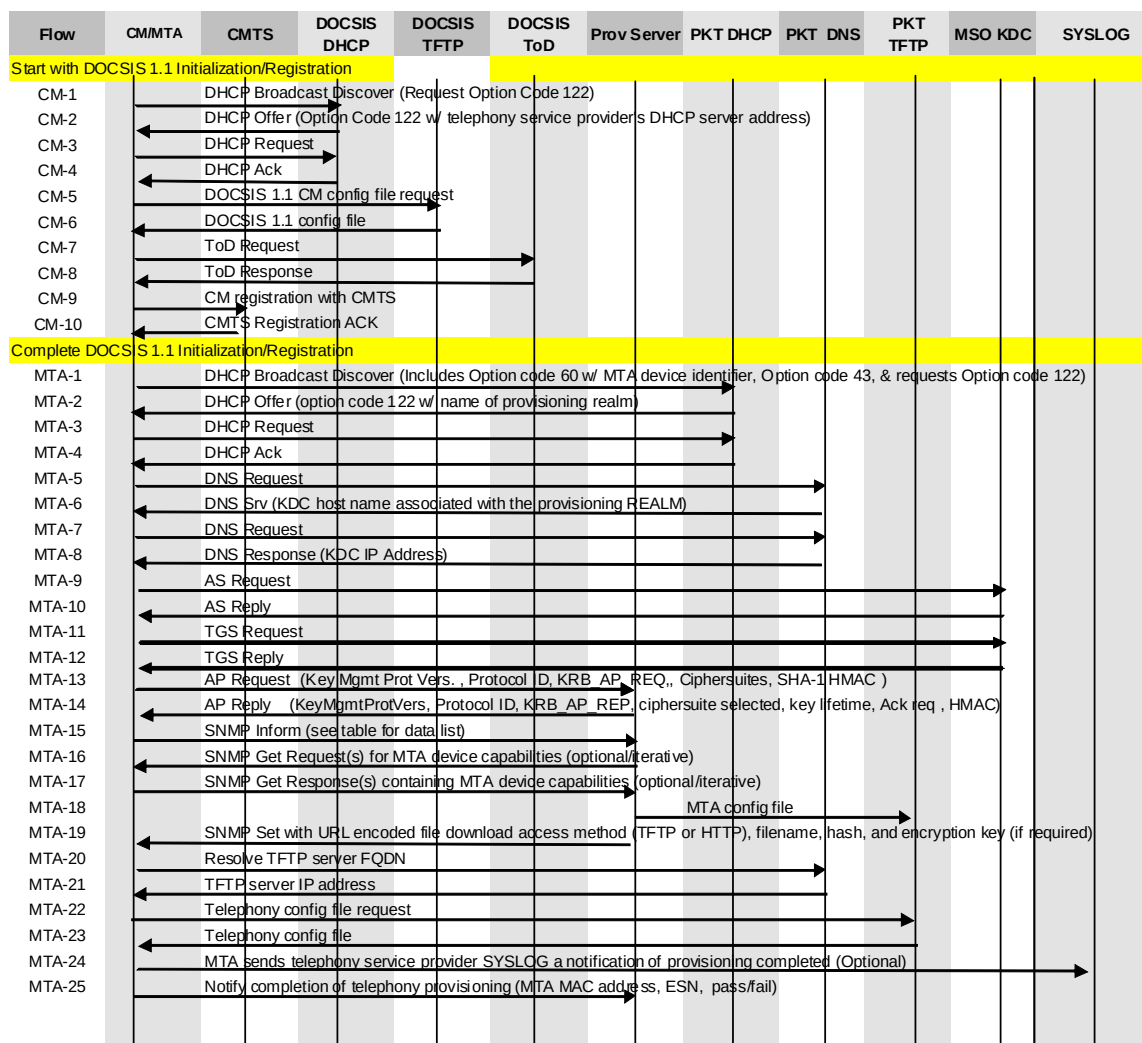


Figure 6 – Embedded-MTA secure power-on initialization flow (IPv4 eCM)

Table 1 – Embedded-MTA power-on initialization flow description (IPv4 eCM)

Flow	Embedded-MTA power-on initialization flow description	Normal flow sequencing	MUST proceed to here if this step fails
CM1	The client device begins device registration by having the CM component send a broadcast DHCP discover message. Included in this message is option code 60 (Vendor Specific Option) in the format "docsis1.1:xxxxxxx". This message MUST request option 122 in option 55, the request parameter list. The remainder of this message MUST conform to the DHCP discover data as defined in the DOCSIS Recommendations.	Initial MUST step in sequence	Per DOCSIS
CM2	The DOCSIS DHCP Server, if it has been configured to support MTA devices, MUST include option code 122 with sub-option 1 and, possibly, sub-option 2 as per clause 8.1. If it is configured to prevent the MTA portion of the device from provisioning, then sub-option 1 in option code 122 MUST contain a DHCP server address of value 0.0.0.0. DOCSIS DHCP Servers without any prior knowledge of MTA devices MAY respond with DHCP OFFER without including option 122.	CM2 MUST occur after CM1 completion	Per DOCSIS
CM3	Upon receiving a DHCP OFFER, the CM MUST check for the requested option 122. If it is not present, then it MUST retry the DHCP DISCOVER process (CM1) exponentially for 3 attempts (e.g., 2-, 4-, 8-second intervals). Upon failing to receive any DHCP OFFER with option 122 after the exponential retry mechanism, it MUST consider OFFERs without option code 122 and accept one of them as per the DHCP specification [IETF RFC 2131]. The client device (CM) MUST then send a DHCP REQUEST broadcast message to the DHCP server whose OFFER is accepted as specified in the DHCP specification [IETF RFC 2131].	CM3 MUST occur after CM2 completion	Per DOCSIS
CM4	The DHCP server sends the client device CM component a DHCP ACK message to confirm acceptance of the offered data. Upon receiving the DHCP ACK, the CM MUST check again for option 122. The absence of option 122 in the DHCP ACK message, which was accepted by the CM, implies that it MUST NOT initialize the embedded MTA. The presence of option 122 implies that it MUST initialize the MTA and pass sub-option 1 and, possibly, sub-option 2. If the option content of this DHCP ACK differs from the preceding DHCP OFFER, the option content of this DHCP ACK MUST be treated as authoritative (per [IETF RFC 2131]).	CM4 MUST occur after CM3 completion	Per DOCSIS
CM5-CM10	The client device's CM component completes the remainder of the CM specified registration sequence. This includes downloading the CM configuration file, requesting time of day registration and registering with the CMTS.	CM5-CM10 MUST occur after CM4 completion	Per DOCSIS

Table 1 – Embedded-MTA power-on initialization flow description (IPv4 eCM)

Flow	Embedded-MTA power-on initialization flow description	Normal flow sequencing	MUST proceed to here if this step fails
MTA1	DHCP Broadcast Discover. The MTA MUST send a broadcast DHCP DISCOVER message. This message MUST include option code 60 (Vendor Specific Option) in the format "pktcl.0:xxxxxx". The MTA MUST include the DHCP option code 43 in the DHCP DISCOVER message as defined in clause 8.5. The MTA MUST request in DHCP option 55 the following: 1, 3, 6, 7, 12, 15 and 122 options. If the CM DHCP option code 122 sub-option 1 (passed by the CM to the MTA) contains a DHCP server of value of 0.0.0.0, then the MTA MUST not attempt to provision and MUST remain dormant until it is reinitialized by the CM.	MTA1 MUST NOT occur before completion of CM4	If failure per DHCP protocol, repeat MTA1
MTA2	DHCP OFFER The MTA may receive multiple DHCP OFFERs (during its wait period as per [IETF RFC 2131]). The following requirements apply to the MTA and/or the Provisioning Applications. 1) The MTA MUST only accept a valid DHCP OFFER message. A valid DHCP OFFER MUST be sent by the primary or secondary DHCP servers returned in DHCP option code 122 sub-options 1 and 2 as obtained by the E-MTA via the CM provisioning step CM4. A valid DHCP OFFER MUST also include the following options: 1, 3, 6, 7, 12, 15, 122 with DHCP option 122 sub-options 3 and 6. DHCP option 122 MAY contain the additional sub-options 4, 5, 7, 8 and 9. 2) If the DHCP option 122 sub-option 6 returned by a valid DHCP server indicates that the Basic or Hybrid flow must be performed, the MTA MUST ignore the DHCP option 122 sub-options 4, 5, 7 and 9 if they are present. 3) If the DHCP option 122 sub-option 6 returned by a valid DHCP server indicates that the Basic Flow must be performed, the Provisioning Server MUST include the configuration file location in the 'siaddr' and 'file' fields in the DHCP responses. 4) If the DHCP option 122 sub-option 6 returned by a valid DHCP server indicates the Secure flow must be performed, the MTA MUST process the DHCP option 122 sub-options 4, 5, 7 and 9. The MTA next applies the following rules to the set of valid DHCP OFFERs: a) The MTA MUST check the value of the DHCP option 122 sub-option 3. If all valid OFFERs contain 0.0.0.0 in DHCP option 122 sub-option 3, then the MTA MUST not further the DHCP process and it MUST shut down until it is reinitialized. Otherwise, the MTA MUST further restrict its set of valid OFFERs to those with a non-zero value in the DHCP option 122 sub-option 3.	MTA2 MUST occur after MTA1 completion	If failure per DHCP protocol, return to MTA1

Table 1 – Embedded-MTA power-on initialization flow description (IPv4 eCM)

Flow	Embedded-MTA power-on initialization flow description	Normal flow sequencing	MUST proceed to here if this step fails
MTA2	b) The MTA MUST check the value of the DHCP option 122 sub-option 6 for indication of the Secure Flow. If no valid DHCP OFFER message directs the MTA to the Secure flow, the MTA MUST retry the DHCP DISCOVER process (MTA1) exponentially for 3 attempts (e.g., 2-, 4-, 8-second intervals). Upon failing to receive any valid DHCP OFFER indicating the Secure flow, the MTA MUST select a valid Hybrid Flow DHCP OFFER, or a valid Basic Flow OFFER in that order. If no valid DHCP OFFER is received, the MTA MUST fail the corresponding provisioning flow step. NOTE – In the case of Secure Flow, if an MTA supports TGTs and receives the DHCP option 122 sub-option 7 set to a FALSE value, it MUST NOT request TGTs. If an MTA supports TGTs and receives the DHCP option 122 sub-option 7 set to a TRUE value, it MUST request TGTs. MTAs that do not support TGTs MUST ignore the DHCP option 122 sub-option 7.		
MTA3	DHCP Broadcast REQUEST Once the MTA has selected a valid DHCP OFFER, the MTA MUST send a DHCP REQUEST broadcast message to accept the DHCP OFFER per [IETF RFC 2131].	MTA3 MUST occur after MTA2 completion	If failure per DHCP protocol, return to MTA1
MTA4	DHCP ACK The DHCP server sends a DHCP ACK message to the MTA. The DHCP ACK message MUST include all options and sub-options which had been sent in MTA2 (DHCP OFFER). If the option and sub-option values of this DHCP ACK differ from the preceding DHCP OFFER (MTA2), the option and sub-option values of this DHCP ACK MUST be treated as authoritative (per [IETF RFC 2131]). If the DHCP ACK is not valid as per the criteria established in MTA2, the MTA MUST fail this step. NOTE – The provisioning flow forks into one of three directions as follows: If the MTA4 DHCP ACK indicates the Basic Flow, the MTA MUST proceed to flow step B-MTA-22 described in clause 7.3. If the MTA4 DHCP ACK indicates the Hybrid Flow, the MTA MUST proceed to flow step H-MTA-15 described in clause 7.4. Otherwise, the Secure Flow is indicated and the MTA MUST proceed to step MTA5 below.	MTA4 MUST occur after MTA3 completion	If failure per DHCP protocol, return to MTA1
MTA5	DNS Srv Request The MTA requests the MSO KDC host name for the Kerberos realm.	MTA5 MUST occur after MTA4 completion	MTA1
MTA6	DNS Srv Reply Returns the MSO KDC host name associated with the provisioning REALM.	MTA6 MUST occur after MTA5 completion	MTA1

Table 1 – Embedded-MTA power-on initialization flow description (IPv4 eCM)

Flow	Embedded-MTA power-on initialization flow description	Normal flow sequencing	MUST proceed to here if this step fails
MTA7	DNS Request The MTA now requests the IP Address of the MSO KDC.	MTA7 MUST occur after MTA6 completion	MTA1
MTA8	DNS Reply The DNS Server returns the IP Address of the MSO KDC.	MTA8 MUST occur after MTA7 completion	MTA1
MTA9	AS Request The AS Request message is sent to the MSO KDC to request a Kerberos ticket.	If MTA9 occurs, it MUST occur after MTA8 completion	MTA1 The failure conditions are defined by the security specification [ITU-T J.170]
MTA10	AS Reply The AS Reply Message is received from the MSO KDC containing the Kerberos ticket. NOTE 1 – The KDC must map the MTA MAC address to the FQDN before sending the AS Reply. NOTE 2 – Flows MTA11-MTA12 are optional in some cases, refer to the security specification ([ITU-T J.170]). NOTE 3 – SNMPv3 entity (FQDN) MUST be resolved to an IP address anywhere during flows MTA5 to MTA12. NOTE 4 – If an IP address is provided in the Additional information field of the DNS-SRV response (MTA6), MTA MAY use the same and skip the flows MTA7 and MTA8. NOTE 5 – If the MTA has valid provisioning application server ticket saved in NVRAM, then it MUST skip the flows MTA5 to MTA12 in successive MTA resets (flows MTA1 to MTA25).	MTA10 MUST occur after MTA9 completion	MTA1
MTA11	TGS Request If MTA obtained TGT in MTA10, the TGS Request message is sent to the MSO KDC.	If MTA11 occurs, it MUST occur after MTA10 completion	MTA1
MTA12	TGS Reply The TGS Reply message is received from the MSO KDC.	MTA12 MUST occur after MTA11 completion	MTA1
MTA13	AP Request The AP Request message is sent to the Provisioning Server to request the keying information for SNMPv3.	MTA13 MUST occur after MTA12 or MTA10 completion	MTA1 The failure conditions are defined by the security specification [ITU-T J.170]

Table 1 – Embedded-MTA power-on initialization flow description (IPv4 eCM)

Flow	Embedded-MTA power-on initialization flow description	Normal flow sequencing	MUST proceed to here if this step fails
MTA14	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.	MTA14 MUST occur after MTA13 completion	MTA1
MTA15	SNMP Enrolment INFORM The MTA MUST send an SNMPv3 Enrollment INFORM to the PROV_SNMP_ENTITY (specified in the DHCP option 122 sub-option 3). The SNMP INFORM MUST contain a "PktcMtaDevProvisioningEnrolment" object as defined in [ITU-T J.166]. The PROV_SNMP_ENTITY notifies the Provisioning Application that the MTA has entered the management domain. NOTE – The provisioning server can reset the MTA at this point in the flows. The MTA is part of the security domain and MUST respond to management requests, the SNMP INFORM of MTA15 is the indicator, see clause 5.4.1.2.	MTA15 MUST occur after MTA14 completion	If failure per SNMP protocol, return to MTA1. SNMP server MUST send response to SNMP-INFORM.
MTA16	SNMPv3 GET Request (Optional). If any additional MTA device capabilities are needed by the PROV_APP, the PROV_APP requests these from the MTA 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 MTA one or more SNMPv3 GET requests to obtain any needed MTA capability information. The Provisioning Application may use a GETBulk request to obtain several pieces of information in a single message.	MTA16 is optional, can occur after MTA15 completion	N/A
MTA17	SNMPv3 GET Response Iterative: MTA sends the PROV_SNMP_ENTITY a response for each GET Request. After all the Gets, or the GetBulk, finish, the PROV_SNMP_ENTITY sends the requested data to the PROV_APP.	MTA17 MUST occur after MTA16 completion if MTA16 is performed	N/A
MTA18	This Protocol is not defined by IPCablecom. The PROV_APP MAY use the information from MTA16 and MTA17 to determine the contents of the MTA Configuration Data file. Mechanisms for sending, storing and, possibly, creating the configuration file are outlined in MTA19.	MTA18 SHOULD occur after MTA15 completion unless MTA16 is performed, then it SHOULD be after MTA17 has completed	N/A

Table 1 – Embedded-MTA power-on initialization flow description (IPv4 eCM)

Flow	Embedded-MTA power-on initialization flow description	Normal flow sequencing	MUST proceed to here if this step fails
MTA19	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 MTA. The PROV_APP MUST store the configuration file on the appropriate TFTP server. The PROV_APP then instructs the PROV_SNMP_ENTITY to send an SNMP SET message to the MTA containing the following variables (defined in [ITU-T J.166]). pkteMtaDevConfigFile pkteMtaDevProvConfigHash and pkteMtaDevProvConfigKey (This MUST NOT be included if the MTA configuration file is unencrypted). NOTE 1 – In the case of file download using the HTTP access method, the filename MUST be URL-encoded with a URL format compliant with [IETF RFC 2616] with the exception stated below in Note 3. NOTE 2 – In the case of file download using the TFTP access method, the filename MUST be URL-encoded with a URL format compliant with [IETF RFC 3617] with the exception stated below in Note 3. NOTE 3 – MTA MUST accept IPv4 addresses embedded in URL encoded format with or without square brackets.	MTA19 MUST occur after MTA18 completion	If failure per SNMP protocol, return to MTA1
MTA20	DNS Request If the URL-encoded access method contains a FQDN instead of an IPv4 address, the MTA MUST use the service provider network's DNS server to resolve the FQDN into an IPv4 address of either the TFTP Server or the HTTP Server.	MTA20 MUST occur after MTA19 completion if FQDN is used	If failure per DNS protocol, return to MTA1
MTA21	DNS Reply DNS Response: DNS server returns the IP address against MTA20 DNS request.	MTA21 MUST occur after MTA20 completion if FQDN is used	If failure per DNS protocol, return to MTA1
MTA22	TFTP/HTTP Configuration file Request The MTA MUST perform either the TFTP or HTTP protocol exchange, as specified in step MTA19, to download its configuration file. For specific details of each protocol, see [IETF RFC 3415] and [IETF RFC 3412].	MTA22 MUST occur: After MTA19 if DNS resolution is not required. After MTA21 if DNS resolution is required.	If failure per TFTP or HTTP protocols, return to MTA1

Table 1 – Embedded-MTA power-on initialization flow description (IPv4 eCM)

Flow	Embedded-MTA power-on initialization flow description	Normal flow sequencing	MUST proceed to here if this step fails
MTA23	TFTP/HTTP Configuration file Request The TFTP/HTTP Server MUST send the requested configuration file to the MTA. Specific details of each protocol are found in [IETF RFC 3415] and [IETF RFC 3412]. The hash of the downloaded configuration file is calculated by the MTA and compared to the value received in step MTA19. If the hashes do not match, the MTA MUST fail this step. If encrypted, the configuration file MUST be decrypted. Refer to clause 9.1 for MTA configuration file contents.	MTA23 MUST occur after MTA22 completion	If the configuration file download failed per TFTP or HTTP protocols, return to MTA1. Otherwise, proceed to MTA24 or MTA25, and send the failed response if the MTA configuration file itself is in error.
MTA24	SYSLOG Notification If a SYSLOG server is configured and enabled as part of the Provisioning Process (Refer to step MTA2 for DHCP Options and ITU-T Rec. J.172, [ITU-T J.166] and [IETF-draft-eventness] for configuration using the MEM-MIB), then the MTA MUST send the voice service provider's SYSLOG a "provisioning complete" event indicating the status of the provisioning operation. This notification will include the pass-fail result of the provisioning operation. The general format of this notification is as defined in clause 5.4.3.	MTA24 MUST occur after MTA23 completion if SYSLOG is configured	The MTA MAY retry this step before proceeding to MTA25
MTA25	SNMP INFORM The MTA MUST send the PROV_SNMP_ENTITY (specified in DHCP option 122 sub-option 3) an SNMP INFORM containing a "provisioning complete" notification. The receipt of the inform is acknowledged by the response message as defined in [IETF RFC 3414]. The SNMP INFORM MUST contain a "pktnMtaDevProvisioningStatus" MIB object. NOTE 1 – At this stage, the MTA device provisioning data is sufficient to provide any minimal services as determined by the service provider (e.g., 611). NOTE 2 – Depending on the TLV-38 configuration, there might be multiple SNMP INFORMs sent to the configured SNMP Management stations.	MTA25 MUST occur after MTA24 if SYSLOG is used, otherwise MUST occur after MTA23 completion	MTA MAY generate a Provisioning Failure event notification to the Service Provider's Fault Management server. Provisioning process stops; manual interaction required. SNMP server MUST send response to SNMP-INFORM.