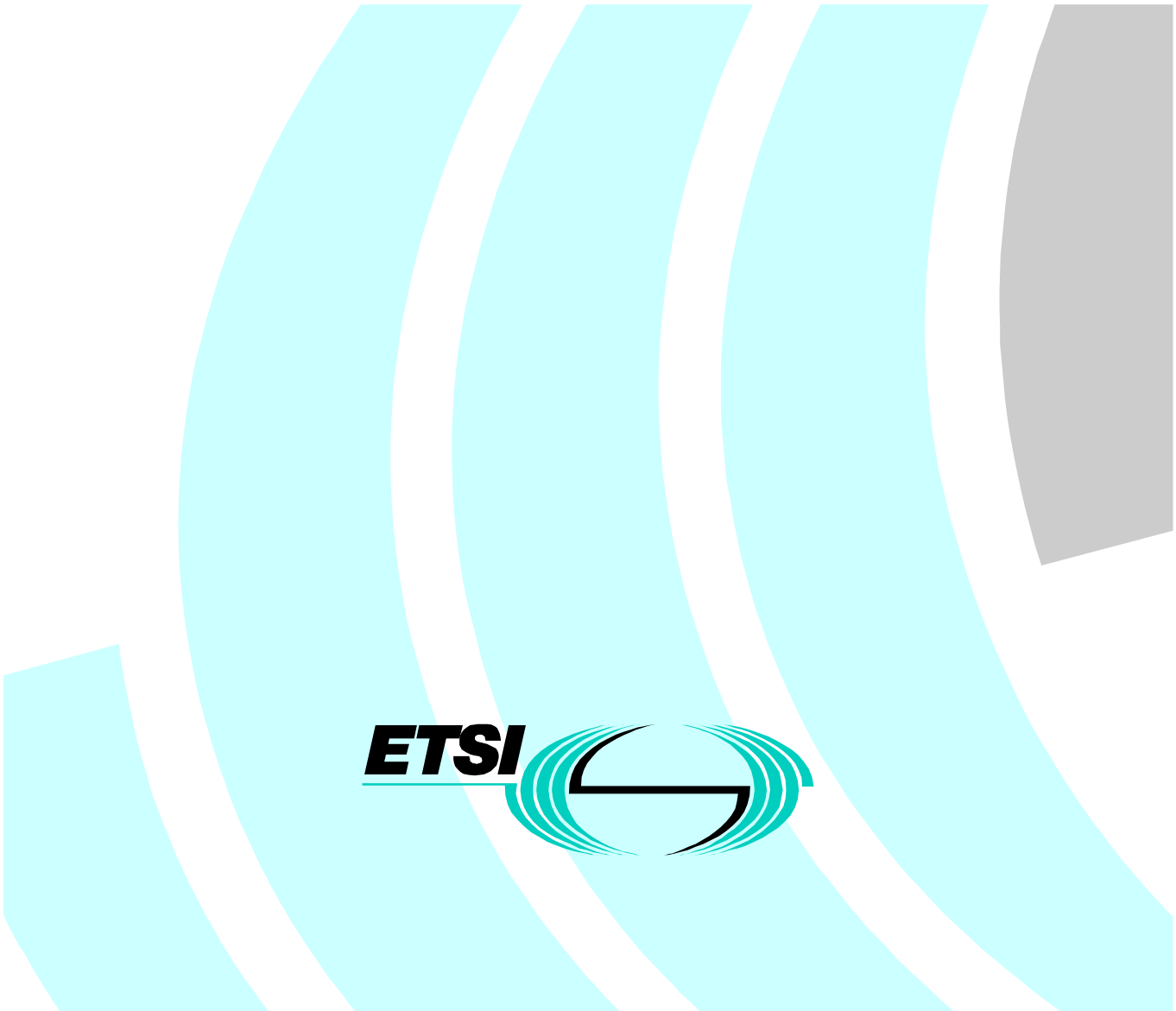
ETSI TS 101 909-6 V1.1.1 (2001-06)

Technical Specification

Access and Terminals (AT);
Digital Broadband Cable Access to the Public Telecommunications Network;
IP Multimedia Time Critical Services;
Part 6: Media Terminal Adapter (MTA) device provisioning



Reference
DTS/AT-020020-06

Keywords
access, broadband, cable, IP, multimedia, PSTN

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Access and Terminals (AT).

The present document is part 6 of a multi-part deliverable supporting real-time multimedia services, as identified below:

Part 1: "General";

Part 2: "Architectural framework for the delivery of time critical services over cable Television networks using cable modems";

Part 3: "Audio Codec Requirements for the Provision of Bi-Directional Audio Service over Cable Television Networks using Cable Modems";

Part 4: "Network Call signalling Protocol";

Part 5: "Dynamic Quality of Service for the Provision of Real Time Services over Cable Television Networks using Cable Modems";

Part 6: "Media Terminal Adapter (MTA) device provisioning";

Part 7: "Management Information Base (MIB) Framework";

Part 8: "Media Terminal Adapter (MTA) Management Information Base (MIB)";

Part 9: "Network Call Signalling (NCS) MIB Requirements";

Part 10: "Event Message Requirements for the Provision of Real Time Services over Cable Television Networks using Cable Modems";

Part 11: "Security";

Part 12: "Internet Signalling Transport Protocol";

Part 13: "Trunking Gateway Control Protocol";

Part 14: "Operation System Support".

NOTE 1: The above list is complete for the first version of this Technical Specification (TS) (V1.1.1 2001-06). Additional parts are being proposed and these will be added to the list in future versions.

The present part is part 6 of the above-mentioned series of ETSI deliverables and describes the IPCablecom MTA device initialization and provisioning process for an embedded MTA device. The present document part also defines the format of the configuration file used for MTA device provisioning. It is limited to the provisioning of an IPCablecom embedded-MTA device by a single provisioning and network management provider.

NOTE 2: The choice of a multi-part format for this deliverable is to facilitate maintenance and future enhancements.

Introduction

The cable industry in Europe and across other Global regions have already deployed broadband cable television hybrid fibre coax (HFC) data networks running the Cable Modem Protocol. The cable industry is in the rapid stages of deploying IP Voice and other time critical multimedia services over these broadband cable television networks.

The cable industry has recognized the urgent need to develop ETSI Technical Specifications aimed at developing interoperable interface specifications and mechanisms for the delivery of end to end advanced real time IP multimedia time critical services over bi-directional broadband cable networks.

IPCablecom is a set of protocols and associated element functional requirements developed to deliver Quality-of-Service (QoS) enhanced secure IP multimedia time critical communications services using packetized data transmission technology to a consumer's home over the broadband cable television Hybrid Fibre/Coaxial (HFC) data network running the Cable Modem protocol. IPCablecom utilizes a network superstructure that overlays the two-way data-ready cable television network. While the initial service offerings in the IPCablecom product line are anticipated to be Packet Voice, the long-term project vision encompasses packet video and a large family of other packet-based services.

The cable industry is a global market and therefore the ETSI standards are developed to align with standards either already developed or under development in other regions. The ETSI Specifications are consistent with the CableLabs/PacketCable set of specifications as published by the SCTE. An agreement has been established between ETSI and SCTE in the US to ensure, where appropriate, that the release of PacketCable and IPCablecom set of specifications are aligned and to avoid unnecessary duplication. The set of IPCablecom ETSI specifications also refers to ITU-SG9 draft and published recommendations relating to IP Cable Communication.

The whole set of multi-part ETSI deliverables to which the present document belongs specify a Cable Communication Service for the delivery of IP Multimedia Time Critical Services over a HFC Broadband Cable Network to the consumers home cable telecom terminal. "IPCablecom" also refers to the ETSI working group program that shall define and develop these ETSI deliverables.

1 Scope

The present set of documents specify IPCablecom, a set of protocols and associated element functional requirements. These have been developed to deliver Quality-of-Service (QoS), enhanced secure IP multimedia time critical communication services, using packetized data transmission technology to a consumer's home over a cable television Hybrid Fibre/Coaxial (HFC) data network.

NOTE 1: IPCablecom set of documents utilize a network superstructure that overlays the two-way data-ready cable television network, e.g. as specified within ES 201 488 and ES 200 800.

While the initial service offerings in the IPCablecom product line are anticipated to be Packet Voice and Packet Video, the long-term project vision encompasses a large family of packet-based services. This may require in the future, not only careful maintenance control, but also an extension of the present set of documents.

NOTE 2: The present set of documents aims for global acceptance and applicability. It is therefore developed in alignment with standards either already existing or under development in other regions and in International Telecommunications Union (ITU).

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

RFC 821 (1982): "Simple Mail Transfer Protocol".

RFC 1157 (1990): "A Simple Network Management Protocol (SNMP)".

RFC 2131: "Dynamic Host Configuration Protocol".

RFC 2132 (1997): "DHCP Options and BOOTP Vendor Extensions".

ETSI TS 101 909-2: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 2: Architectural framework for the delivery of time critical services over cable Television networks using cable modems".

ETSI TS 101 909-4: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 4: Network Call signalling Protocol".

ETSI TS 101 909-5: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 5: Dynamic Quality of Service for the Provision of Real Time Services over Cable Television Networks using Cable Modems".

ETSI TS 101 909-8: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 8: Media Terminal Adaptor (MTA) Management Information Base (MIB)".

ETSI TS 101 909-9: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 9: Network Call Signalling (NCS) MIB Requirements".

ETSI TS 101 909-11: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 11: Security".

ETSI ES 201 488: "Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification".

ETSI ES 200 800: "Digital Video Broadcasting (DVB); DVB interaction channel for Cable TV distribution systems (CATV)".

ITU-T Recommendation J.112: "Transmission systems for interactive cable television services".

ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Access Node: layer two termination device that terminates the network end of the ITU-T Recommendation J.112 connection

NOTE: It is technology specific. In ITU-T Recommendation J.112, annex A, it is called the INA while in annex B it is the CMTS.

Cable Modem: layer two termination device that terminates the customer end of the J.112 connection

IPCablecom: ETSI working group project that includes an architecture and a series of Specifications that enable the delivery of real time services (such as telephony) over the cable television networks using cable modems

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AN	Access Node
CM	Cable Modem
CMS	Call Management Server
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Naming System
FQDN	Fully Qualified Domain Name
HFC	Hybrid Fibre/Coaxial
HTTP	HyperText Transfer Protocol
IP	Internet Protocol
IPSEC	Internet Protocol Security
MAC	Media Access Control
MTA	Media Terminal Adaptor
QoS	Quality of Service
PSTN	Public Switched Telephone Network
SNMP	Signalling Network Management Protocol
TFTP	Trivial File Transfer Protocol
TGS	Ticket Granting Server

4 Overview of the IPCablecom system and goals

4.1 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 ITU-T Recommendations J.83 and J.112. This is shown in simplified form in Figure 1.

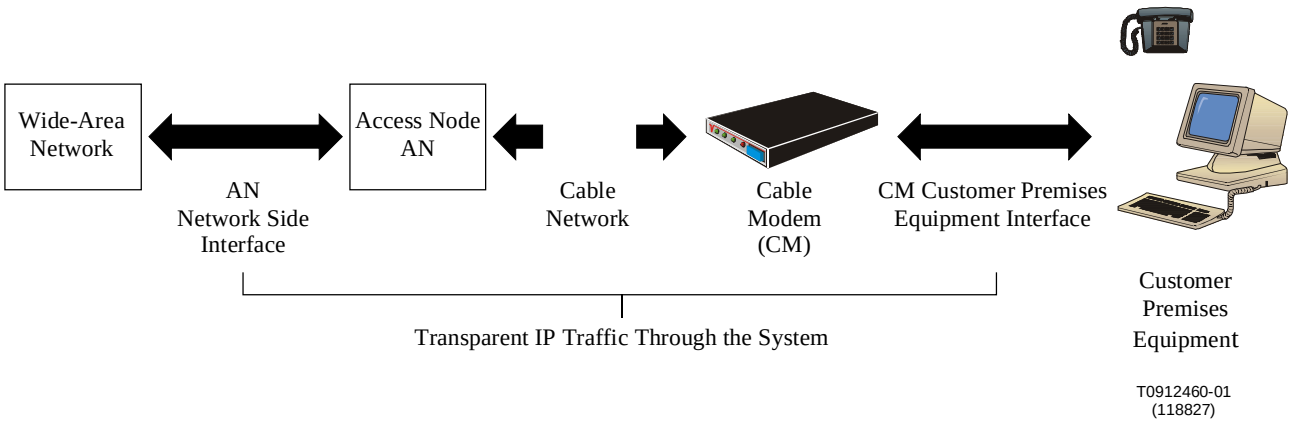


Figure 1: Transparent IP Traffic Through the Data-Over-Cable System

The transmission path over the cable system is realized at the headend by an Access Node (AN), and at each customer location by a CM.

4.2 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.
- An embedded-MTA is a IPCablecom MTA combined with a CM. Both CM and IPCablecom device provisioning steps MUST be performed for this embedded-MTA device to be provisioned. The embedded-MTA MUST have two IP addresses; an IP address for the CM component and a different IP address for the MTA component. The embedded-MTA MUST have two MAC addresses, one MAC address for the CM component and a different MAC address for the MTA-component.
- IPCablecom requires a unique FQDN for the MTA-component in the embedded-MTA. This FQDN MAY be included in the DHCP offer to the MTA-component. IPCablecom makes no additional FQDN requirements on the CM component in the embedded-MTA beyond those required by ITU-T Recommendation J.112. If the FQDN is NOT included in the DHCP offer, then the FQDN MUST be included in the MTA configuration file and mapping of the FQDN to IP address MUST be configured in the network DNS server and be available to the rest of the network.
- IPCablecom embedded-MTA provisioning MUST support two separate configuration files, an ITU-T Recommendation J.112 specified configuration file for the CM component and a IPCablecom-specified configuration file for the MTA component.
- The embedded-MTA is outside the IPCablecom network trust boundary as defined in the IPCablecom architecture document TS 101 909-2.
- The CM software download process supports the downloading of the software image to the embedded MTA.
- IPCablecom MUST support use of SNMPv3 security for network management operations.
- IPCablecom embedded-MTA provisioning minimizes the impact to ITU-T Recommendation J.112 devices (CM and AN) in the network.
- Standard server solutions (TFTP, SNMP, DNS, etc.) must be supported. It is understood that an application layer may be required on top of these protocols to co-ordinate IPCablecom embedded-MTA provisioning.
- Where appropriate, the ITU-T Recommendation J.112 management protocols are supported.

4.3 IPCablecom Reference Architecture

Figure 2 shows the reference architecture for the IPCablecom Network. Refer to the architecture document ETSI TS 101 909-2 for more detailed information on this reference architecture.

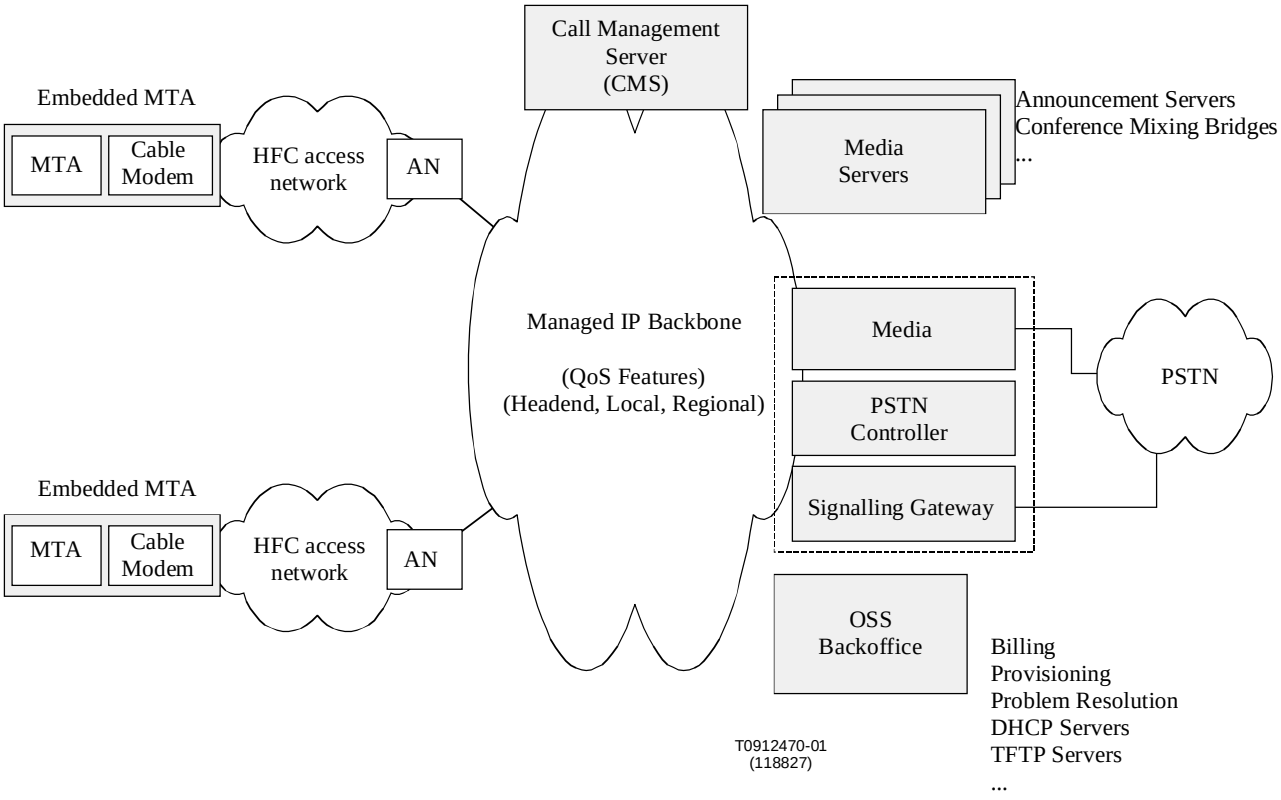


Figure 2: IPCablecom Network Component Reference Model (partial)

4.4 Components and Interfaces

The basic IPCablecom embedded-MTA provisioning reference architecture is shown in Figure 3. This figure represents the components and interfaces discussed in the present document.

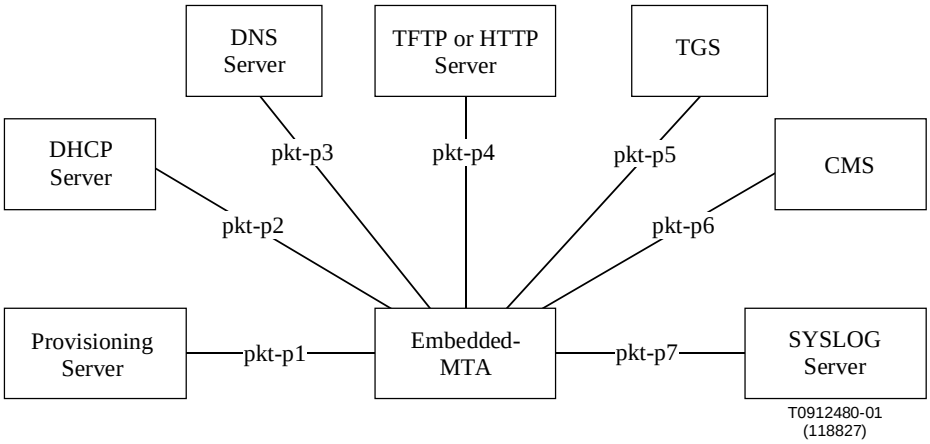


Figure 3: IPCablecom Provisioning Interfaces

4.4.1 MTA

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

4.4.1.1 MTA Security Requirements

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

- The MTA MUST generate a random number that will be exchanged as part of the device capability data to the Provisioning Application. This mechanism is referred to as "using nonce". This mechanism is required to ensure correctness of the provisioning configuration data file downloaded to the MTA. The nonce MUST be regenerated every time the MTA power-on initialization occurs.

- The MTA MUST generate a correlation number 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 MTA MUST obtain an MTA Telephony Certificate (X.509 certificate) for each network operator's Call Management Server(s) (CMS) assigned to an MTA's voice communications endpoint. This certificate MUST be provided to the MTA as part of the MTA's provisioning data. If the MTA Telephony certificate was issued by a Local System CA, then the corresponding Local System Certificate MUST also be provided. Please refer to TS 101 909-11 for further information. If the MTA Telephony certificate was issued by a Local System CA, then the corresponding Local System Certificate MUST also be provided.

- The MTA MUST obtain a Service Provider Certificate (X.509 certificate) from the network operator that "owns" the CMS assigned to an MTA's voice communications endpoint. This certificate MUST be provided to the MTA as part of the MTA's provisioning data.

- The MTA MUST fail the provisioning operation if ever a CMS is assigned to an MTA's voice communications endpoint without the MTA having been provisioned with both the MTA Telephony Certificate and the Telephony Service Provider Certificate.

- The MTA MUST fail provisioning operation if ever one of its endpoints is assigned an MTA Telephony Certificate that is signed by a Local System CA and the corresponding Local System Certificate is not provisioned for that endpoint.

- The MTA device MIB is structured to represent the assignment of an MTA endpoint to a CMS. However, the security association between an MTA and a CMS is on a per-device basis.

- For each unique pair of CMS Kerberos principal Name/Kerberos Realm assigned to an endpoint, the MTA MUST obtain a single Kerberos ticket per TS 101 909-11.

- 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 <= 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 (inbound and outbound) 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. (RFC 2131)

- During the MTA initialization, 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.

4.4.1.2 MTA SNMPv3 Requirements

The MTA MUST conform to the following SNMPv3 requirements during the 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 setup separately.

- SNMPv3 initialization MUST be completed prior to the provisioning enrolment inform.

- SNMPv3 security will not be available until after successful processing of the configuration file.

4.4.2 Provisioning Server

The Provisioning Server is made up of the following components:

- Provisioning Application - The Provisioning Application is responsible for co-ordinating the embedded-MTA provisioning process. This application has an associated SNMP Entity.
- Provisioning SNMP Entity - The provisioning SNMP entity includes a trap handler for provisioning enrolment and the provisioning status traps as well as an SNMP engine for retrieving device capabilities and setting the TFTP filename and access method. Refer to the IPCablecom MTA MIB TS 101 909-8 for a description of the MIB accessible MTA attributes.

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.

4.4.3 Telephony Syslog Server

The IPCablecom Telephony Syslog server allows the MTA to report network or device events.

4.4.4 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 code 60 and DHCP option code 177 as defined in the present document.
- The DHCP server MUST accept and support broadcast and unicast messages from the MTA DHCP client.
- The DHCP server MAY include the MTA's assigned FQDN in the DHCP offer message to the MTA-component of the embedded-MTA. Refer to RFC 2132 for details describing the DHCP offer message.

4.4.5 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 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 provide secure SNMP access to the device.
- The Provisioning Application MUST support online incremental device/subscriber provisioning using SNMP with security enabled.

4.4.6 MTA to CMS

Signalling is the main interface between the MTA and the CMS. Refer to the IPCablecom signalling document TS 101 909-4 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.

4.4.7 MTA to Security Server (TGS)

The interface between the MTA and the Ticket Granting Server (TGS) MUST conform to the IPCablecom security specification TS 101 909-11.

4.4.8 MTA and Configuration Data File Access

The present document part 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 device will be provided with the URL-encoded TFTP server address and configuration filename via an SNMPv3 SET from the provisioning server.
- The MTA MAY support HTTP access method for downloading the MTA configuration data file. The device will be provided with the URL-encoded HTTP server address and configuration filename via an SNMPv3 SET from the provisioning server.

4.4.9 DHCP extensions for MTA Provisioning

The present document part requires that the following additions to DHCP be supported for MTA auto-provisioning:

- A new DHCP offer message option code 177 and the associated procedures MUST be implemented in DHCP.

5 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.

5.1 Device Provisioning

Device provisioning is the process by which an embedded-MTA device is configured to support voice communications service. For example, a network provider MAY decide to configure unassociated MTAs to provide a short code service for in-band subscriber enrolment, or possibly emergency service.

In either case, 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.

The MTA device MUST be able to verify the authenticity of the configuration file it downloads from the server. Privacy of the configuration data is also necessary. Thus, the configuration data will be "signed and sealed" by packaging the data into an MTA device sealed object. Please refer to TS 101 909-11 for further information.

Please refer to clause 4.4.1.1 for provisioning rules related to security associations.

5.2 Endpoint Provisioning

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

Device registration will employ the Kerberos CMS Ticket the MTA obtained during subscriber enrolment. Please refer to TS 101 909-11 for further information.

5.3 Provisioning State Transitions

The following 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. Definitions of these logical states are above and beyond ITU-T Recommendation J.112 State definitions, except the DHCP sequence, which is the same for both a CM and an MTA. The following state transitions do not specify the number of retry attempts or retry time out values:

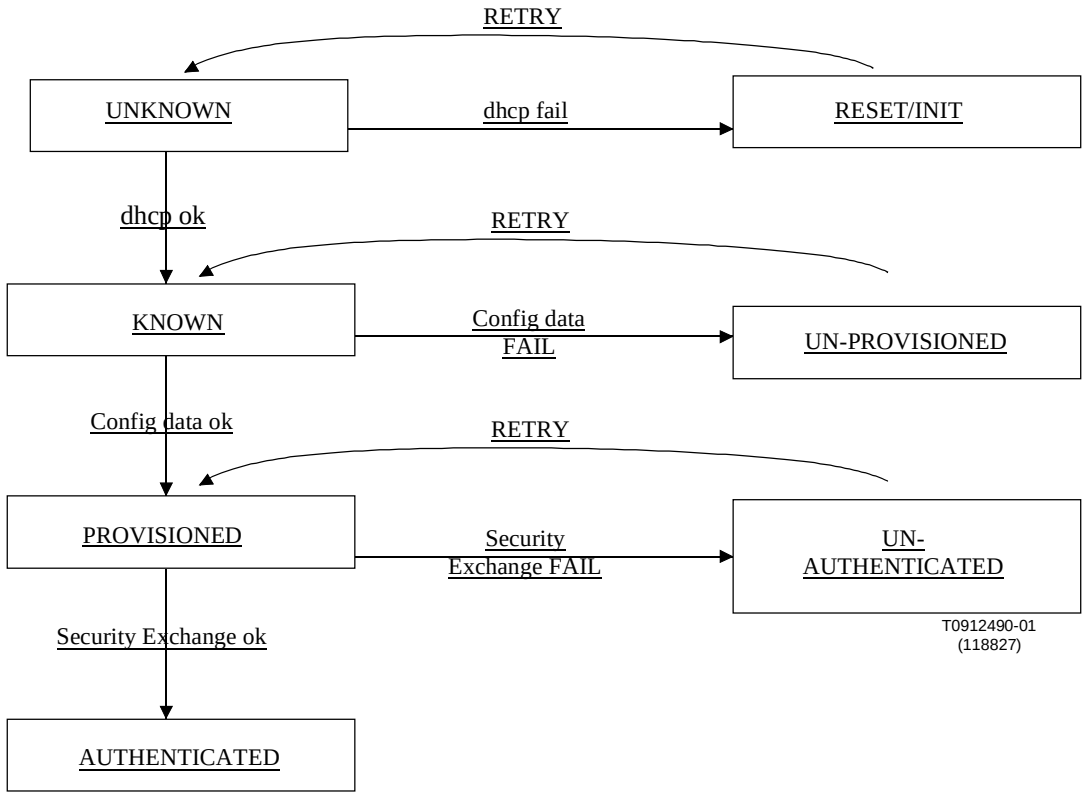


Figure 4: Device States and State Transitions

6 Provisioning Flows

6.1 Backoff, Retries and Timeouts

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 timeout values. The details of provisioning behaviour under mass-registration is beyond the scope of IPCablecom, however this clause provides the following specifications and requirements:

- Throttling of registrations MAY be based on specifications provided by the access network media access control protocol.
- The MTA MUST follow DHCP (RFC 2131) and HTTP specification timeout and retry mechanisms.
- The MTA MUST use an adaptive timeout for TFTP.
- The MTA MUST follow backoff and retry specifications that are defined in the security specification (TS 101 909-11) for the security message flows.

6.2 Embedded-MTA Power-On Initialization Flows

Following is the representative message flow that the embedded-MTA device follows during power-on initialization. Note that these flows are informative and for reference only. 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.

Table 1: Embedded-MTA Power-On Initialization Flow Description

Flow	Embedded-MTA Power-On Initialization Flow Description	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 a device identifier (option code 60) to identify the device as either a CM only device or a CM device with an embedded MTA. The remainder of this message MUST conform to the DHCP discover data as defined in ITU-T Recommendation J.112.	Per Cable DHCP.
CM2	One or more DHCP servers may respond with a DHCP offer message. To be considered a valid DHCP offer for IPCablecom voice communications, the offer message MUST contain the IPCablecom option code 177 with sub-option 1, the offer message MUST contain the IPCablecom option code 177 with sub-option 1 and MAY contain sub-option 2.	Per DHCP.
CM3	The client device MUST select a single DHCP offer that includes the IPCablecom code 177 values as defined in clause 7.1 to function as a IPCablecom voice communications-enabled device. The client device may select the first valid DHCP offer, or it may use its own internal selection rules to determine which valid DHCP offer to accept. The client device sends the appropriate DHCP server a DHCP REQUEST message to accept the DHCP offer. Refer to RFC 2131 for more details concerning the DHCP protocol.	Per DHCP.
CM4	The DHCP server sends the client device CM component a DHCP ACK message to confirm acceptance of the offered data.	Per DHCP.
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 AN.	Per access network MAC protocol.
MTA1	The MTA sends a unicast DHCP DISCOVER message to the DHCP server address specified in the CM-level DHCP Offer Message (Option code 177 from CM2 above). Included in this message is a device identifier (option code 60) to identify the device as a CM device with an embedded MTA. (Refer to clause 7.2.)	Per DHCP protocol.
MTA2	Only the specified DHCP server will respond with a DHCP offer message. This offer will contain the IP address to be used for the client device's MTA component. It will also include the IPCablecom Option Code 177 with sub-option 2 and optionally sub-options 3 and 4 if the network is DNS-enabled.	Per DHCP protocol.
MTA3	The client device's MTA component MUST select this DHCP offer. The client device's MTA component MUST select a DHCP offer as specified in sub-options 1 and 2 sent in CM-2. If sub-option 1 contains 255.255.255.255, then the MTA uses logic defined in DHCP (RFC 2132) to select an offer. Otherwise, the MTA MUST only accept an offer specified by the DHCP server(s) in sub-options 1 and 2. The MTA component sends the appropriate DHCP server a DHCP REQUEST message to accept the DHCP offer. Refer to RFC 2131 for more details concerning the DHCP protocol.	Per DHCP protocol.

Flow	Embedded-MTA Power-On Initialization Flow Description	Proceed to here if this step fails
MTA4	The DHCP server sends the client device's MTA component a DHCP ACK message which MUST contain the IPv4 address of the MTA and MAY contain the FQDN to confirm acceptance of the offered data. (see note 1)	Per DHCP protocol.
MTA5	The client device MTA component sends the PROV_SNMP_ENTITY an SNMPv3 INFORM requesting enrolment. The IP address of this PROV_SNMP_ENTITY is contained in the IPCablecom DHCP offer message. As defined in the security spec TS 101 909-11, the MTA MUST create a randomly generated nonce and include the nonce in the MTA device signature. The following information MUST be in the "PktcMtaProvisioningEnrolment" object: • Hardware Version; • Software Version; • Device Identifier String (EMTA:PKTC1.0:CM:xxxxxx); • MAC address; • Telephony Provisioning Correlation ID; • MTA device signature (includes randomly generated nonce value). This is used for authentication. Refer to the security document part TS 101 909-11 for more details. Please refer to the "PktcMtaProvisioningEnrolment" object in the MTA MIB (TS 101 909-8) for a detailed description of these data values. The PROV_SNMP_ENTITY notifies the PROV_APP that the MTA has entered the management domain. (see notes 2, 3 and 4)	MTA5
MTA6	(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. Each PROV_SNMP_ENTITY SNMP Get command MUST encapsulate the SNMPv3 message using the MTA Device signature obtained from the provisioning enrolment inform, with the exception of the SNMPv3 Get Requests to get the MTA device certificate and MTA Manufacturer certificate. Refer to the security specification TS 101 909-11 for handling of the SNMPv3 get commands for the MTA device certificate and MTA Manufacturer certificate.	MTA6
MTA7	Iterative: MTA sends the PROV_SNMP_ENTITY a Get 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. The MTA device signature in these responses MUST include the same nonce value that was originally included in the corresponding SNMPv3 INFORM message.	MTA6
MTA8	The PROV_APP uses the information to determine the contents of the MTA Configuration Data file and creates the configuration file at this point. The PROV_APP stores the configuration file on the appropriate TFTP server. The configuration file is signed by the PROV_APP with the "Prov Server's private key" and sealed with the "MTA's public key", using an MTA device signature wrapper defined in the security specification. The nonce value included in this MTA device signature MUST be the same nonce value that was sent by the MTA in the corresponding SNMP INFORM message in flow MTA-5.	MTA8
MTA9	The PROV_APP then instructs the PROV_SNMP_ENTITY to send an SNMP Set message to the MTA containing the URL-encoded file access method and filename (i.e. tftp:<filename>). (see note 5)	MTA9

Flow	Embedded-MTA Power-On Initialization Flow Description	Proceed to here if this step fails
MTA10 - MTA11	If the URL-encoded access method contains a FQDN instead of an IPv4 address, the MTA will 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.	MTA10
MTA12	The MTA sends the TFTP Server a TFTP Get Request to request the specified configuration data file. (see note 6)	MTA12
MTA13	The TFTP Server sends the MTA a TFTP Response containing the requested file. In the case of file download using the HTTP access method, the HTTP server sends the MTA a response containing the requested file. Refer to clause 9.2 for MTA configuration file contents. (see notes 7 and 8) Enable SNMPv3 security if no error condition occurred during this step. If IPCablecom and CM share the same SNMPv3 manager, then the SNMPv3 kickstart for CM MUST already have been enabled and MUST also have enabled SNMPv3 security for IPCablecom and no additional IPCablecom SNMPv3 security actions are required. Otherwise, SNMPv3 security for IPCablecom MUST be enabled in this step.	Repeat MTA13 if the configuration file download failed. Otherwise, proceed to MTA14 and send the failed response if the MTA configuration file itself is in error.
MTA14	The MTA sends the voice service provider's SYSLOG (identified in the configuration data file) a "provisioning complete" notification. This notification will include the pass-fail result of the provisioning operation. The general format of this notification is as defined in the CM Device MIB specification details on syslog events.	A vendor MAY consider returning to MTA5, repeating until it is determined to be a hard failure and then MUST continue to MTA15.
MTA15	The MTA MUST send the PROV_SNMP_ENTITY an SNMP INFORM containing a "provisioning complete" notification. The following information MUST be in the "PktcMtaProvisioningStatus" object: • MAC address; • Telephony Provisioning Correlation ID; • MTA device signature (includes randomly generated nonce value); • Provisioning State (PASS or FAIL).	MTA MAY generate a Provisioning Failure event notification to the Service Provider's Fault Management server. Provisioning process stops; Manual interaction required.
	NOTE: The following security flows are only performed for the first endpoint provisioned with this CMS Name. If another endpoint on this MTA already has an active security association with the specified CMS, then the following steps MUST NOT be performed:	
Get Kerberos tickets associated with each CMS with which the MTA communicates. (see note 9)		
SEC1	For each different CMS assigned to voice communications endpoints, the MTA requests a Kerberos Ticket for the CMS by sending a PKINIT REQUEST message to the TGS containing the MTA Telephony Certificate (specified in the MTA configuration file), the MTA FQDN and the assigned CMS Identifier.	
SEC2	The TGS sends the MTA a PKINIT REPLY message containing the CMS Kerberos Ticket for the assigned CMS.	
Establish IPSEC security association between the MTA and each CMS with which the MTA communicates. (see note 10)		
SEC3	The MTA requests a pair of IPSEC simplex Security Associations (inbound and outbound) with the assigned CMS by sending the assigned CMS a Kerberos AP REQUEST message containing the CMS Kerberos Ticket.	
SEC4	The CMS establishes the Security Associations by sending an AP REPLY message with the corresponding IPSEC parameters.	

Flow	Embedded-MTA Power-On Initialization Flow Description	Proceed to here if this step fails
SEC5	(Required during error conditions - refer to security specification TS 101 909-11 for error handling.) The MTA responds with an "SA Recovered message" that lets the CMS know, the MTA is now ready to receive on its incoming IPSEC Security Association.	

NOTE 1: The FQDN MUST be available in the device before Kerberos Ticket generation can occur.
NOTE 2: The Telephony Provisioning Correlation ID is a numeric value that is used to correlate the configuration download notification insteps MTA-14 and MTA-15 with this enrolment request.
NOTE 3: Both the MTA device signature and the nonce MUST be regenerated every time this step occurs.
NOTE 4: SNMPv3 initialization MUST have occurred prior to the sending of this information.
NOTE 5: In the case of file download using the HTTP access method, the URL-encoded filename is: http:://{IPv4 or FQDN of access server}/ mta-config-filename.
NOTE 6: In the case of file download using the HTTP access method, the MTA sends the HTTP server a request for the specified configuration data file.
NOTE 7: At this stage, the MTA device provisioning data is sufficient to provide any minimal services as determined by the service provider (e.g. 611, 911).
NOTE 8: SNMPv3 authentication and privacy keys are included in this configuration file. These keys are used to turn on IPCablecom SNMPv3 security with both message integrity and privacy on all subsequent SNMP messages.
NOTE 9: SEC1 and SEC2 MUST be repeated for each CMS with which the MTA communicates.
NOTE 10: SEC3, SEC4 and SEC5 MUST be repeated for each CMS with which the MTA communicates.

6.3 Post Initialization Incremental Provisioning

This clause describes the flows allowing the Provisioning Application to perform incremental provisioning of individual voice communications endpoints after the MTA has been initialized and authenticated. Post-Initialization incremental provisioning MAY involve communication with a Customer Service Representative (CSR).

6.3.1 Synchronization of Provisioning Attributes with Configuration File

Incremental provisioning includes adding, deleting and modifying subscriber services on one or more endpoints of the embedded-MTA. Services on an MTA endpoint MUST be modified using SMNPv3 via the MTA MIB (TS 101 909-8). The back office applications MUST support a "flow-through" provisioning mechanism that synchronizes all device provisioning information on the embedded-MTA with the appropriate back office databases and servers. Synchronization is required in the event that provisioning information needs to be recovered in order to re-initialize the device. Although the details of the back office synchronization are beyond the scope of the present document part, it is expected that, at a minimum, the following information be updated: customer records and the MTA configuration file on the TFTP or HTTP server.

6.3.2 Enabling Services on an MTA Endpoint

Services may be provisioned on a per-endpoint basis whenever it is desired to add or modify service to a previously unprovisioned endpoint. This would be the case if a customer was already subscribing to service on one or more lines (endpoints) and now wanted to add additional service on another line (endpoint).

MTA Endpoint services are enabled using SMNPv3 via the MTA MIB (TS 101 909-8). In this example, a subscriber is requesting that additional service be added. This example assumes the service provider's account creation process has been completed, and shows only the applications critical for the flows. For instance, account creation and billing database creation are assumed to be available and integrated in the back office application suite.

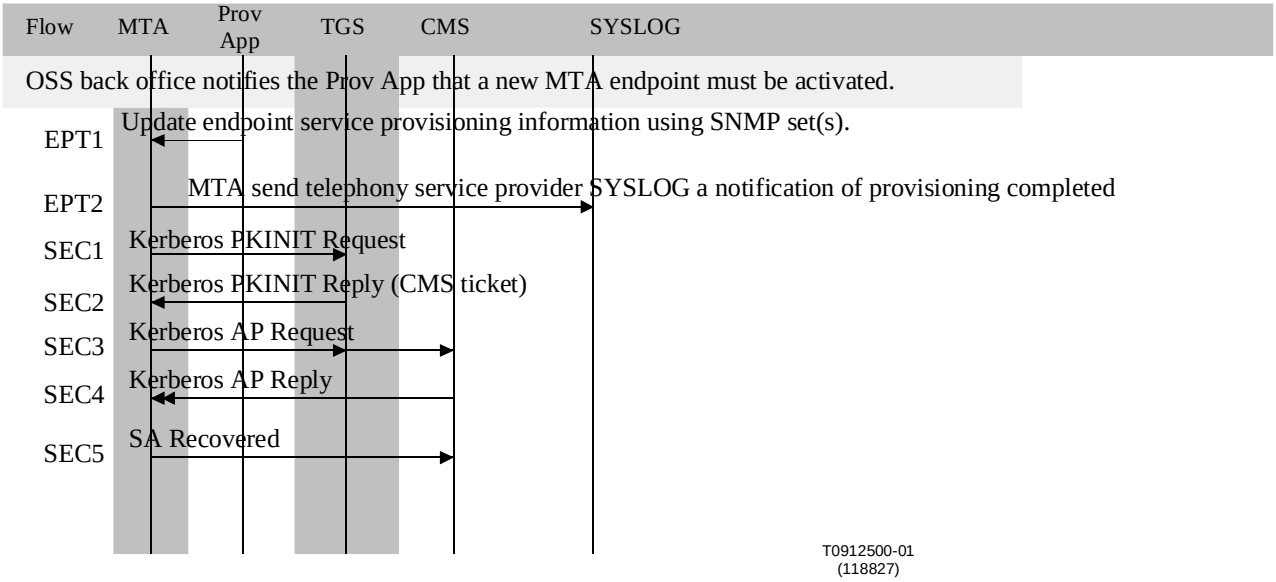


Figure 5: Enabling Services on an MTA Endpoint

Table 2: Enabling Services on an MTA Endpoint Flow Description

Flow	Enabling Services on an MTA Endpoint Flow Description
EPT1	The Provisioning Application will now use SNMP Sets to update provisioning attributes on the device for which the device port is being enabled. These SET operations MUST include the device port CMS ID (associate the device port to the CMS ID from which the features will be supported), the device port to enable and the MTA IP Telephony Certificate from the selected service provider. See clause 4.4.1 for details of provisioning rules.
EPT2	The MTA sends the service provider's SYSLOG (identified in the configuration data file) a "provisioning complete" notification. This notification will include the pass-fail result of the provisioning operation. The general format of this notification is as defined in the CM Device MIB specification details on syslog events.
	NOTE: The following security flows assume that this is the first endpoint provisioned with this CMS Name. If another endpoint on this MTA already has an active security association with the specified CMS, then the following steps MUST NOT be performed.
SEC1	For each different CMS assigned to voice communications endpoints, the MTA requests a certificate for the CMS by sending a PKINIT REQUEST message to the TGS containing the MTA Telephony Certificate, the MTA FQDN and the assigned CMS Identifier.
SEC2	The TGS sends the MTA a PKINIT REPLY message containing the CMS Kerberos Ticket for the assigned CMS.
SEC3	The MTA requests a security association with the assigned CMS by sending the assigned CMS a Kerberos AP REQUEST message containing the CMS Kerberos Ticket.
SEC4	The CMS establishes the security association by sending an AP REPLY message with the IPSEC Security Association parameters.
SEC5	(Required during error conditions - refer to security specification TS 101 909-11 for error handling.) The MTA responds with an SA Recovered message that lets the CMS know the MTA is now ready to receive on its incoming IPSEC Security Association.

6.3.3 Disabling Services on an MTA Endpoint

MTA Endpoint services are disabled using SMNP Sets to the MTA. In this scenario, subscriber's voice communications service is disabled from one of the MTA endpoints. This example assumes the service provider's account update process has been completed and shows only the applications critical to MTA operation.

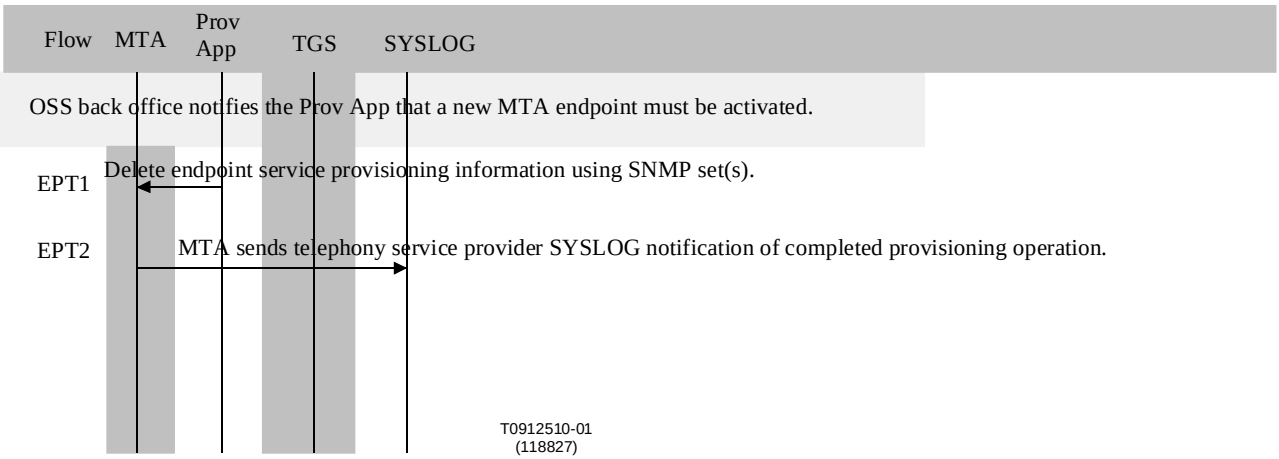


Figure 6: Disabling Services on an MTA Endpoint

Table 3: Disabling Services on an MTA Endpoint

Flow	Disabling Services on an MTA Endpoint Flow Description
EPT1	The Provisioning Application will now use SNMP Sets to delete provisioning attributes from the device endpoint for which the service is being disabled. This MUST include setting the associated security parameters to a NULL value.
EPT2	The MTA sends the service provider's SYSLOG (identified in the configuration data file) a "provisioning complete" notification. This notification will include the pass-fail result of the provisioning operation. The general format of this notification is as defined in the CM Device MIB specification details on SYSLOG events.

6.3.4 Modifying Services on an MTA Endpoint

MTA Endpoint services are modified using SMNPv3 Sets to the MTA MIB (TS 101 909-8). In this scenario subscriber's voice communications service features are being modified on one of the MTA endpoints. Once again, the accounting management aspects of the back office application are assumed to be correct.

The following are possible service modifications and none of these modifications cause the device to recreate the subscriber ticket from the TGS system:

1) Modification of call service features (add, delete call features). Changes to services require modifications in the CMS, not in the MTA.

2) Modification of service level (change the subscriber service levels with respect to the QoS definition). This is part of the CM provisioning and requires changes to the CM component in the MTA which requires rebooting the embedded-MTA. This updates the MTA (CM) as the initialization sequence is executed as part of the bootup process.

6.4 MTA Replacement

The initialization sequence for the replaced MTA will be the same as the MTA's first-time initialization described in clause 6. Once the MTA is initialized, an additional step is required by the network management system to move the profile from the old MTA to the new MTA. The subscriber account migration can occur with the help of the Customer Service Representative (CSR) provided the CSR can validate the subscriber account information. If the subscriber uses Interactive Voice Response (IVR) and Web-Based Enterprise Management (WBEM) systems to migrate profiles from the old MTA to the new MTA, the IVR and WBEM systems are expected to validate the subscriber identification and allow profile migration process.

The detailed process for migrating subscriber profiles from the old MTA to the new MTA is beyond the scope of the present document.

The initialization flow as described in clause 6 will apply for the replaced MTA. If the replaced MTA is new or if the replaced MTA has registered once, then all the above-described flows are applicable.

6.5 Temporary Signal Loss

The treatment for RF loss in the MTA MUST be similar to that of a CM. Therefore, if the RF loss at the MTA is sufficient to cause the MTA to reinitialize, then the MTA is required to repeat the initialization sequence described in clause 6.

7 DHCP Options

DHCP is used to obtain IPv4 addresses for both the CM and the MTA. The DHCP option code 60 and option code 177 described in the table below MUST be supported during the CM and the MTA DHCP messages.

7.1 Code 177: IPCablecom Servers Option

DHCP option code 177 is a temporary code that the IPCablecom embedded-MTA device can use until a permanent code is assigned by the IETF. Refer to the power-on initialization flows in clause 6 for further details.

DHCP option code 177 is used in both the CM and MTA DHCP OFFER messages to identify a list of valid IPCablecom network servers. The IPCablecom servers are identified using either an IPv4 address or a FQDN. Each sub-option of DHCP option code 177 identifies a particular type of IPCablecom server. Refer to RFC 2132 section 2 for DHCP encoding and formatting details.

During the CM device provisioning sequence of an embedded-MTA, the sub-option 1 MUST and sub-option 2 MAY be included in the CM's DHCP OFFER message. The MTA's DHCP OFFER MUST contain sub-option 3 and MAY contain sub-options 4 and 5. IPCablecom-defined DHCP option fields are encoded in the following format using option code 177:

Table 4: Server Options

Option	Sub-option	Description and Comments
177	1	Service Provider's Primary DHCP Server Address.
	2	Service Provider's SNMP Entity Secondary DHCP Server Address.
	3	Service Provider's SNMP Address.
	4	Service Provider Network Primary Domain Name Server.
	5	Service Provider Network Secondary Domain Name Server.

The following clauses provide detailed descriptions of each sub-option of DHCP option code 177. Note that UDP port numbers are normally standard values as defined in RFC1340. However, the format of the sub-option data fields defined here have a provision to optionally include port numbers for these systems if a port number other than the standard is required. If no port number is specified, the standard port number based on the definitions in RFC 1340 is assumed. For example, the standard DNS UDP port number is 42/udp.

7.1.1 Service Provider's DHCP Server Address (sub-option 1 and sub-option 2)

The Service Provider's DHCP Server Address identifies the DHCP server that will be used to obtain an MTA-unique IP address for a given service provider's network administrative domain.

The Service Provider's DHCP Server Address identifies the DHCP servers that a DHCP Offer will be accepted from to obtain an MTA-unique IP address for a given service provider's network administrative domain.

These addresses are configured as IPv4 addresses. If sub-option 1 contains 255.255.255.255, then the MTA uses logic defined in DHCP to select an Offer. Otherwise, the MTA MUST only accept an Offer specified by the DHCP server(s) in sub-option(s) 1 and 2.

Sub-option 1 MUST be included in the DHCP Offer to the CM and indicates the Primary DHCP server or 255.255.255.255. The value of 255.255.255.255 specifies that the MTA MAY use its own criteria in selecting a DHCP Offer. Sub-option 2 MAY be used to identify a redundant or backup DHCP server.

The encoding of sub-option 1 is as follows:

Table 5: DHCP Server Address

Option	Sub-option	Value	Comments
177	1	[xxx.xxx.xxx.xxx]:NNNN FQDN:NNNN	The IP address of the Primary DHCP Server where NNNN is an optional UDP port number if different from the well-known port defined in RFC 1350.
177	2	[xxx.xxx.xxx.xxx]:NNNN	The IP address of the Secondary DHCP Server where NNNN is an optional UDP port number if different from the well-known port defined in RFC 1350.

7.1.2 Service Provider's SNMP Entity Address (sub-option 3)

The Service Provider's SNMP Entity Address is the network address of the default server for a given voice service provider's network administrative domain. The Service Provider's SNMP Entity Address component MUST be capable of accepting SNMP traps.

This address can be configured as either an FQDN or as an IPv4 address. Since FQDN and IPv4 are of two different formats, a syntax was chosen which allows a way of specifying either address attribute as a DISPLAYSTRING. The syntax for this method is shown in the table below. Refer to RFC 821 for additional details concerning the syntax for this bracketed IP address notation.

The encoding of sub-option 3 is as follows:

Table 6: SNMP Entity Address

Option	Sub-option	Value	Comments
177	3	[xxx.xxx.xxx.xxx]:NNNN FQDN:NNNN	Either the IPv4 address or the FQDN will be configured. Where NNNN is an optional UDP port number if different from the well-known port defined in RFC 1340.

7.1.3 DNS system (sub-option 4 and sub-option 5)

The Service Provider's DNS server is required to resolve an IPCablecom device's FQDN into an IPv4 address. The DNS server's address MUST be specified in the IPv4 format.

Sub-option 4 is the address of the network's primary DNS server and MUST be specified if option 3 is in FQDN format. Sub-option 5 is the address of the network's secondary DNS server. Sub-option 5 MAY be specified to identify a redundant or backup DNS server.

The encoding syntax for sub-option 4 and sub-option 5 is as follows:

Table 7: DNS system

Option	Sub-option	Value	Comments
177	4	[xxx.xxx.xxx.xxx]:NNNN	This field is the IPv4 address of the service provider's primary DNS server. Where NNNN is an optional UDP port number if different from the well-known port defined in RFC 1350.
177	5	[xxx.xxx.xxx.xxx]:NNNN	This field is the IPv4 address of the service provider's secondary DNS server. Where NNNN is an optional UDP port number if different from the well-known port defined in RFC 1350.

7.2 Code 60: Vendor Client Identifier

Option code 60 contains encoded ASCII values representing the type of IPCablecom MTA. Possible values are for an embedded MTA and for future use a stand-alone MTA. Both the CM-component and the MTA-component of an embedded-MTA MUST encode this option in their DHCP discover messages. The following table shows the IPCablecom extensions to the DHCP option 60 requirements.

Table 8: Vendor Client Identifier

Option	Length	Value	Comments
60	30	EMTA:PKTC1.0:Yyyyyyy:xxxxxxx	The CM-component and the MTA-component encodes option 60 in the DHCP messages. Where PKTC stands for IPCablecom and EMTA refers to embedded MTA and SMTA refers to Stand-alone MTA. The suffix xxxxxxx is defined by the access network protocol. The yyyyyyy is to be replaced by the corresponding access network protocol.
		EMTA:PKTC:Yyyyyyy:xxxxxxx	
		SMTA:PKTC1.0:Yyyyyyy:xxxxxxx (for future use)	
		SMTA:PKTC1.1:Yyyyyyy:xxxxxxx (for future use)	

8 MTA Provisionable Attributes

This clause includes the list of attributes and their associated properties used in device provisioning. All of the provisionable attributes specified in this clause MAY be updated via the MTA configuration data file, or on a per-attribute basis using SMNP with security.

IPCablecom requires that an MTA configuration data file MUST be provided to all embedded-MTAs during the registration sequence. If no voice services are enabled at the time of device initialization, the configuration data file MUST include all Device Level Configuration Data to explicitly configure device level information as desired by the network service provider. These items are contained in the table defined in clause 8.2.1.

8.1 MTA Configuration File Name

The MTA configuration data filename generated by the Provisioning Application MUST be less than 255 bytes in length and cannot be NULL. Since this filename is provided to the MTA by the Provisioning Application during the registration sequence, it is not necessary to specify a file naming convention.

8.2 MTA Configuration File

The following is a list of attributes and their syntax for objects included in the MTA configuration file. This file contains a series of TLV parameters. Each TLV parameter in the configuration file describes an MTA or endpoint attribute. The configuration data file includes TLVs that have read-write, read only, and no MIB access. Unless specifically indicated, all MIB-accessible configuration file parameters MUST be defined using TLV type 11 as shown below.

Type (1byte)	Length (1byte)	Value
11	n	variable binding

where the value is an SNMP VarBind as defined in RFC 1157. The VarBind is encoded in ASN.1 Basic Encoding Rules, just as it would be if part of an SNMP Set request. The use of type 11 TLV-tuplus allows SNMP variables to be set via the MTA configuration file. The CM must treat this object as if it were part of an SNMP Set Request with the following caveats:

1) It must treat the request as fully authorized.

2) SNMP Write Control provisions do not apply.

3) No SNMP response is generated by the CM.

Type 11 may be repeated with different VarBinds to "Set" a number of MIB objects. Further, each VarBind must be limited to 255 bytes.

The MTA configuration file MUST start with the "telephony configuration file start" type and MUST end with the "telephony configuration file end" type. These types are defined in section 6.2.1 of the present document part These tags also provide deterministic indications for start and stop of the MTA configuration file.

The MTA configuration file MUST contain the Device Level Configuration Data. The MTA configuration file MUST be sent to the embedded-MTA every time this device is powered on. The MTA enrolment inform (step MTA-5 of the provisioning flow) is the trigger which causes the configuration file to be sent to the embedded-MTA.

The MTA configuration file MAY contain Device Level Service Data. If the MTA configuration file contains Device Level Service Data, then it MUST contain the attributes identified as "required" in the table below and MAY contain any of the non-required attributes.

The Device Level Service Data MUST be sent to the MTA when voice communications service is activated. The Device Level Service Data MAY be sent to the MTA as part of the MTA configuration file or it MAY be sent to the MTA via SNMP with security. Refer to clause 6.3.1 for a discussion concerning synchronization of provisioning attributes with back office systems.

The MTA configuration file MAY contain Per-Endpoint Configuration Data. If the MTA configuration file contains Per-Endpoint Configuration Data, then, for each MTA endpoint, the file MUST contain the attributes identified as "required" in the table below and MAY contain any of the non-required attributes. The Per-Endpoint Configuration Data MUST be sent to the MTA when voice communications service is activated. The Per-Endpoint Configuration Data MAY be sent to the MTA as part of the MTA configuration file or it MAY be sent to the MTA via SNMP with security. Refer to clause 6.3.1 for a discussion concerning synchronization of provisioning attributes with back office systems.

Authentication of the MTA configuration file MUST be supported via the MTA-generated nonce sent in the SNMP Inform. If the MTA configuration file can NOT be authenticated, then the MTA configuration file MUST be discarded.

8.2.1 Device Level Configuration Data

Refer to the MTA MIB (TS 101 909-8) for more detailed information concerning these attributes and their default values.

- The MTA Manufacturer Certificate validates the MTA Device Certificate.

Table 9: Device Level Configuration

Attribute	Syntax	Configuration Access	SNMP Access	Comments
Telephony Config File Start	Integer	W, required	None	Type length value 254 1 1 The MTA config file MUST start with this attribute.
Telephony Config File End	Integer	W, required	None	Type length value 254 1 255 This MUST be the last attribute in the MTA config file.
Telephony MTA Admin State	ENUM	W, required	R/W	Used to enable/disable all telephony ports on the MTA. Applies to the MTA side of the embedded-MTA or the entire stand-alone MTA. Allows blanket management of all telephony ports (external interfaces) on the device. Enabled - allows all telephony ports to manage traffic carrying capability on an individual basis. Disabled - disallows traffic carrying capability of all MTA telephony endpoints. Telephony call setup requests, and post-power-on-provisioning SNMP sets will be rejected by the MTA while in a disabled state. Therefore, this attribute MUST be enabled before SNMP per-endpoint provisioning can occur.
IPCablecom MTA Device FQDN	String	W, required (refer to note 1)	R/W	Fully Qualified Domain Name for this Device. (see note 1)
Telephony Service Provider SNMP Entity	String	W, required	R/W	This attribute is the FQDN or IPv4 address of the MTA's SNMP Entity. The MTA MUST reject the MTA config file if this value is not provided. If this value is NULL in the MTA config file, then the value provided in DHCP 177 sub-option 2 of the CM-component ITU-T Recommendation J.112 DHCP offer MUST be used.
Telephony Service Provider DHCP Server	String	W, required	R/W	This attribute is the FQDN or IPv4 address of the MTA DHCP Server. This attribute identifies the DHCP server to which the MTA requests IPv4 address lease renewals. If this value is NULL in the MTA config file, then the value provided in DHCP 177 sub-option 1 of the MTA-component ITU-T Recommendation J.112 DHCP offer MUST be used.
Telephony Provider Syslog Server	String	W, required	R/W	This attribute is the FQDN or IPv4 address of the MTA system log server. If this value is 0.0.0.0, then it implies that syslog logging for the MTA is turned off.
IPCablecom Telephony Provisioning Correlation ID	Integer 32	W, required	R/O	Arbitrary value generated by the MTA for use in registration authorization. It is for use only in the MTA initialization messages and for MTA configuration file download.
MTA Privacy Key	String	W, required	None	MTA Privacy Key - MTA config file attribute (NOT in MIB). A unique 16 byte string created by the Provisioning

Attribute	Syntax	Configuration Access	SNMP Access	Comments
				Application and used by the MTA and the Provisioning Application to derive the SNMPv3 encryption key for this MTA. There must be a separate SNMPv3 management user for each MTA. Refer to RFC 2574 (see Bibliography). The MTA Privacy key does not need to be on a per-endpoint basis (i.e. multiple endpoints can share the same key).
MTA Authentication Key	String	W, required	None	MTA Authentication Key - MTA config file attributes (NOT in MIB). A unique 16 byte string created by the Provisioning Application and used by the MTA and the Provisioning Application to establish SNMPv3 security and authenticate messages. (Used in MTA-13.)
USM User Name	String	W, required	None	The name of the user. This is used as the index to the other USM information. (see note 2)
USM User Authentication Protocol	ENUM	W, required	R/W	This specifies the authentication protocol used in SNMPv3 messages.
USM User Privacy Protocol	ENUM	W, required	R/W	This specifies the privacy protocol used in SNMPv3 messages.
MTA Device Certificate	String	W, required	R/O	MTA Device Certificate - The MTA's X.509 public-key certificate installed in the embedded-MTA by the manufacturer.
MTA Manufacturer Certificate	String	W, required	R/O	MTA Manufacturer Certificate - The MTA Manufacturer's X.509 public-key certificate. This certificate is required to validate the MTA's Device Certificate.
MTA Device Signature	String	W, required	R/W	MTA Device Signature - A unique signature created by the MTA for each SNMP Inform or SNMP Trap or SNMP GetResponse message exchanged (MTA-5 and MTA-7) prior to enabling SNMPv3 security. The MTA Digital Signature is in the Cryptographic message syntax, ASN.1 encoded.
NOTE 1: If the FQDN is NOT included in the DHCP offer, then the FQDN MUST be included in the MTA configuration file and mapping of the FQDN to IP address MUST be configured in the network DNS server and be available to the rest of the network. NOTE 2: This object is an MIB table index.				

8.2.2 Device Level Service Data

Refer to the MTA MIB (TS 101 909-8), the NCS MIB (TS 101 909-9), the NCS Call Signalling specification (TS 101 909-4) and RFC 2131 for more detailed information concerning these attributes and their default values.

Table 10: Device Level Service

Attribute	Syntax	Configuration Access	SNMP Access	Comments
NCS Default Call Signalling TOS	Integer	W, required	R/W	The default value used in the IP header for setting the TOS value for NCS call signalling.
NCS Default Media Stream TOS	Integer	W, required	R/W	The default value used in the IP header for setting the TOS value for NCS media stream packets.
NCS TOS Format Selector	ENUM	W, required	R/W	The format of the default NCS signalling and media TOS values. Allowed values are "IPv4 TOS octet" or "DSCP codepoint". Refer to IETF RFC 2131.
R0 cadence	Bit-field	W, required	R/W	User defined bit field where each bit represents a duration of 200 ms (6 s total) 1 = active ringing, 0 = silence. If this field is not going to be used, it MUST be set to zero.
R6 cadence	Bit-field	W, required	R/W	User defined bit field where each bit represents a duration of 200 ms (6 s total) 1 = active ringing, 0 = silence. If this field is not going to be used, it MUST be set to zero.
R7 cadence	Bit-field	W, required	R/W	User defined bit field where each bit represents a duration of 200 ms (6 s total) 1 = active ringing, 0 = silence. If this field is not going to be used, it MUST be set to zero.

8.2.3 Per-Endpoint Configuration Data

Refer to the NCS MIB TS 101 909-9, the NCS spec TS 101 909-4, the security spec TS 101 909-11 and the MTA MIB TS 101 909-8 for more detailed information concerning these attributes and their default values.

- MTA sends TGS the MTA/CMS certificate, MTA's FQDN, CMS-ID. The TGS returns the MTA a "Kerberos Ticket" that says "this MTA is assigned to this CMS".
- The Telephony Service Provider Certificate validates the MTA Telephony Certificate.
- If two different endpoints share the same CMS FQDN then all six security-attributes MUST be identical: Kerberos Realm, CMS Kerberos Principal Name, PKINIT grace period, TGS name list, MTA IP telephony certificate, telephony service provider certificate. If a Local System Certificate is present, it too MUST be the same for both endpoints.
- If two different endpoints share the same Kerberos Realm and same CMS Kerberos Principal Name, then these four attributes MUST be identical: PKINIT grace period, TGS name list, MTA telephony certificate, telephony service provider certificate. If a Local System Certificate is present, it too MUST be the same for both endpoints.

Table 11: Per-Endpoint Configuration

Attribute	Syntax	Access	SNMP Access	Comments
Port Admin State	ENUM	W, required	R/W	The administrative state of the port the operator can access to either enable or disable service to the port. The administrative state can be used to disable access to the user port without de-provisioning the subscriber. Allowed values for this attribute are: Enabled/disabled. For SNMP access it is found in the ifTable of MIB-II.
Call Management Server Name	String	W, required	R/W	This attribute is the FQDN or IPv4 address of the CMS assigned to the endpoint. DNS support is assumed to support multiple CMSs as described in the NCS spec.
Call Management Server UDP Port	Integer	W	R/W	UDP port for the CMS.
Partial Dial Timeout	Integer	W	R/W	Timeout value in seconds for partial dial timeout.
Critical Dial Timeout	Integer	W	R/W	Timeout value in seconds for critical dial timeout.
Busy Tone Timeout	Integer	W	R/W	Timeout value in seconds for busy tone.
Dial tone timeout	Integer	W	R/W	Timeout value in seconds for dialtone.
Message Waiting timeout	Integer	W	R/W	Timeout value in seconds for message waiting.
Off Hook Warning timeout	Integer	W	R/W	Timeout value in seconds for off hook warning.
Ringing Timeout	Integer	W	R/W	Timeout value in seconds for ringing.
Ringback Timeout	Integer	W	R/W	Timeout value in seconds for ringback.
Reorder Tone timeout	Integer	W	R/W	Timeout value in seconds for message waiting.
Stutter dial timeout	Integer	W	R/W	Timeout value in seconds for message waiting.
TS Max	Integer	W	R/W	Contains the maximum time in seconds since the sending of the initial datagram.
Max1	Integer	W	R/W	The suspicious error threshold for each endpoint retransmission.
Max2	Integer	W	R/W	The disconnect error threshold per endpoint retransmission.
Max1 Queue Enable	Enum	W	R/W	Enables/disables the Max1 DNS query operation when Max1 expires.
Max2 Queue Enable	Enum	W	R/W	Enables/disables the Max2 DNS query operation when Max2 expires.
MWD	Integer	W	R/W	Number of seconds to wait to restart after a restart is received.
Tdinit	Integer	W	R/W	Number of seconds to wait after a disconnect.
TDMin	Integer	W	R/W	Minimum number of seconds to wait after a disconnect.
TDMax	Integer	W	R/W	Maximum number of seconds to wait after a disconnect.
RTO Max	Integer	W	R/W	Maximum number of seconds for the retransmission timer.
RTO Init	Integer	W	R/W	Initial value for the retransmission timer.
Long Duration Keepalive	Integer	W	R/W	Timeout in minutes for sending long duration call notification messages.
Thist	Integer	W	R/W	The timeout period in seconds before no response is declared.
Telephony Service Provider Kerberos Realm	String	W, required	R/W	String that identifies a collection of CMS and TGS servers.

Attribute	Syntax	Access	SNMP Access	Comments
Telephony Service Provider Certificate	String	W, required	R/W	The Telephony Service Provider's X.509 public-key certificate given to all MTAs who have signed up with the given Telephony Service Provider.
Local System Certificate	String	W	R/W	X.509 public key certificate of the Local System CA. This certificate is present if, and only if, the MTA Telephony Certificate for this endpoint is signed by a Local System CA (instead of the Service Provider CA).
MTA Telephony Certificate	String	W, required	R/W	The MTA's X.509 public-key certificate that allows this MTA to register with any Kerberos Server in any realm belonging to the given Telephony Service Provider. (MUST contain the MTA's IPv4 or FQDN assigned by the Telephony Service Provider.) (see note)
Call Management Server Kerberos Principal Name	String	W, required	R/W	Identifies a collection of CMSs or a CMS cluster that share the same TGS and also share the same "Kerberos ticket". This information is required in order for the MTA to obtain Call Management Server Kerberos tickets. This principal name does not include the realm, which is specified as a separate field in this configuration file. A single Kerberos principal name MAY be shared among several Call Management Servers.
TGS Name List	String	W, required	R/W	List of FQDN or IPv4 of this endpoint's TGS server(s). There may be multiple entries of this type. The order in which these entries are listed is the priority order in which the MTA will attempt to contact them.
PKINIT Grace Period	Integer	W	R/W	# minutes before the "Kerberos Ticket" assigned to this endpoint expires that the MTA must obtain a new "Kerberos Ticket" from the TGS Name List. If two endpoints share the same Kerberos Ticket, then both endpoints must have the same PKINIT grace period value. The MTA MUST obtain a new Kerberos ticket (with a PKINIT exchange) this many minutes before the old ticket expires.
NOTE: If this certificate contains the MTA's IPv4 address, then any time the IPv4 address changes, the Telephony Service Provider MUST issue the MTA a new certificate.				

9 MTA Device Capabilities

MTA device capabilities information is contained in a combination of MIBs including: IETF's MIB-II, the MTA MIB the NCS MIB and the CM CableDevice MIB. Use of capabilities information by the Provisioning Application is optional. Examples of capabilities information includes:

Table 12: MTA Device Capabilities

Attribute
HTTP Download File Access Method Supported
Echo Cancellation
Silence suppression
Connection mode
Device Serial Number
MAC
Number of Endpoints
Supported Codec Types
MTA Device Identifier
Active Software Version
Backup Software Version

Annex A (informative): Bibliography

PacketCable Vendor specific DHCP option, a PacketCable proposal to the IETF DHCP Committee. Primary Author Burcak Baser 3COM.

Cable Modem to Customer Premise Equipment Interface Specification, CMCI, DOCSISAN SP-CMCI-I02-980317, Cable Television Laboratories, Inc.

Cable Modem Termination System - Network Side Interface Specification, Cable Television Laboratories, Inc., July 22, 1996, http://www.CableLabs.com/.

Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification, SP-RFIv1.1-I03-991105, Cable Television Laboratories, Inc., November 05, 1999, http://www.CableLabs.com/.

PacketCable Provisioned QoS Specification**,** PKT-SP-PQoS-D02-990603, June 18, 1999, Cable Television Laboratories, Inc.

Operations Support System Interface Specification Radio Frequency Interface, sp-ossi-rfi-i03-990113, Cable Television Laboratories, Inc., January 13, 1999, http://www.CableLabs.com/.

RFC 1034 (1987): "STD 13 Domain Names - Concepts and Facilities".

RFC 1035 (1987): "Domain Names - Implementation and Specifications".

RFC 1123 (1989): "Braden, R., Requirements for Internet Hosts - Application and Support".

RFC 1340 (1992): "Assigned Numbers" (contains ARP/DHCP parameters).

RFC 1350 (1992): "The TFTP Protocol (Revision 2)", STD 33, RFC 1350, MIT.

RFC 1449: "Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)".

RFC 1591 (1994): "Domain Name System Structure and Delegation".

RFC 1903: "Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)".

RFC 1945: "Hypertext Transfer Protocol".

RFC 2349 (1998): "TFTP Timeout Interval and Transfer Size Options".

RFC 2475 (1998): "An Architecture for Differentiated Services".

RFC 2574: "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)".

ETSI TS 101 909-3: "Access and Terminals (AT); Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 3: Audio Codec Requirements For The Provision Of Bi-Directional Audio Service Over Cable Television Networks Using Cable Modems".

ITU-T Recommendation J.83 (1997): "Digital multi-programme systems for television, sound and data services for cable distribution".

List of ITU-T Recommendations referring to IP Cablecom:

ITU-T Recommendation J.160: "Architectural framework for the delivery of time critical services over cable television networks using cable modems".

ITU-T Recommendation J.161: "Audio codec requirements for the provision of bidirectional audio service over cable television networks using cable modems".

ITU-T Recommendation J.162: "Network call signalling (NCS) MIB requirements".

ITU-T Recommendation J.163: "Dynamic quality of service for the provision of real time services over cable television networks using cable modems".

ITU-T Recommendation J.164: "Event Message requirements for the support of real-time services over cable television networks using cable modems".

ITU-T Recommendation J.165: "IPCablecom Internet Signalling Transport Protocol".

ITU-T Recommendation J.166: "IPCablecom Management information base (MIB) framework".

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".

ITU-T Recommendation J.168: "IPCablecom media terminal adapter (MTA) MIB requirements".

ITU-T Recommendation J.169: "IPCablecom network call signalling (NCS) MIB requirements".

ITU-T Recommendation J.170: "IPCablecom Security specification".

ITU-T Recommendation J.171: "IPCablecom Trunking Gateway Control Protocol (TGCP)".

History

Document history		
V1.1.1	June 2001	Publication