PacketCable™ MTA Device Provisioning Specification

PKT-SP-PROV-I01-991201

Interim

Notice

Document Status Sheet

Document Control Number:	PKT-SP-PROV-I01-991201			
Document Title:	PacketCable™ MTA Device Provisioning Specification			
Revision History:	I01-991201: release			
Date:	December 1, 1999			
Status:	~~Work in Progress~~	~~Draft~~	Interim	~~Released~~
Distribution Restrictions:	~~Author Only~~	~~CL/Member~~	~~CL/ PacketCable/ Vendor~~	Public

Key to Document Status Codes:

Work in Progress	An incomplete document designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
Draft	A document in specification format considered largely complete, but lacking reviews by Members and vendors. Drafts are susceptible to substantial change during the review process.
Interim	A document which has undergone rigorous Member and vendor review, suitable for use by vendors to design in conformance to and for field testing. For purposes of the “Contribution and License Agreement for Intellectual Property" which grants licenses to the intellectual property contained in the PacketCable Specification, an "Interim Specification" is a "Published” Specification.
Released	A stable document, reviewed, tested and validated, suitable to enable cross-vendor interoperability.

Contents

Figures

This page intentionally left blank.

INTRODUCTION

1.1 Purpose

This specification describes the PacketCable™ 1.0 embedded-MTA device initialization and provisioning. This specification being issued to facilitate design and testing, addresses the features, manageability, and interoperability of conforming hardware and software by multiple vendors.

1.2 Scope

The scope of this document is limited to the provisioning of a PacketCable 1.0 embedded-MTA device by a single provisioning and network management provider. An attempt has been made to provide enough detail to enable vendors to build an embedded-MTA device that is interoperable in a PacketCable 1.0 network configuration.

1.3 Document Overview

This specification describes provisioning of a PacketCable 1.0 embedded-MTA. The document is structured as follows:

- Section 2 – Background information including a description of the provisioning reference architecture, components and interfaces.
- Section 3 – Provisioning overview including logical state transition diagram.
- Section 4 – Provisioning flows for initial power-on, post-power-on, scenarios involving updating services on an MTA endpoint, and limited failure scenarios.
- Section 5 – PacketCable requirements for DHCP [1] option code 60 and option code 177.
- Section 6 – MTA configuration file
- Section 7 - List of MTA device capabilities.

1.4 Requirements Syntax

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

"MUST": This word or the adjective "REQUIRED" means that the item is an absolute requirement of this specification.

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

"SHOULD": This word 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 behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

"MAY": This word 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. Other text is descriptive or explanatory.

2 BACKGROUND

2.1 Service Goals

Cable operators are interested in deploying high-speed data communications systems on cable television systems. Comcast Cable Communications, Inc., Cogeco, Cox Communications, Tele-Communications, Inc., Time Warner Cable, MediaOne, Inc., Rogers Cablesystems Limited, Le Groupe Vidéotron, and Cable Television Laboratories, Inc. (on behalf of the CableLabs® member companies), have decided to prepare a series of interface specifications that will permit the early definition, design, development, and deployment of packet data over cable systems on an uniform, consistent, open, non-proprietary, multi-vendor interoperable basis. The intended service enables voice communications, video, and data services based on bi-directional transfer of Internet protocol (IP) traffic, between the cable system headend and customer locations, over an all-coaxial or hybrid-fiber/coax (HFC) cable network, defined by the data over cable service interface specification (DOCSIS) standard [16]. This is shown in simplified form in Figure 1.

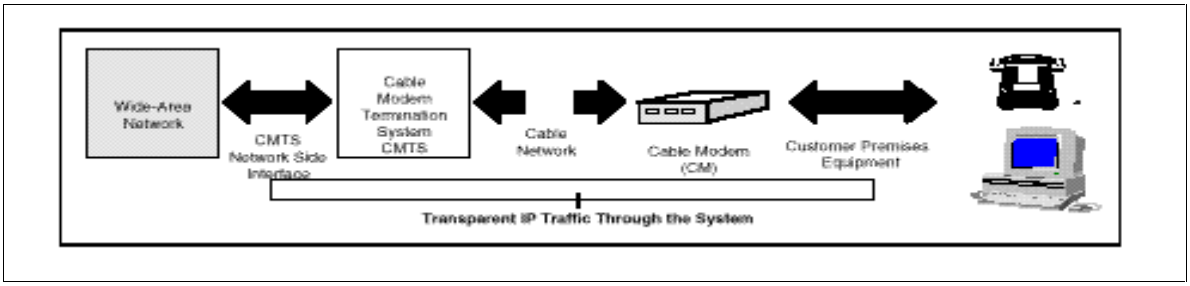


Figure 1. Transparent IP Traffic Through the Data-Over-Cable System

The transmission path over the cable system is realized at the headend by a cable modem termination system (CMTS), and at each customer location by a cable modem (CM). At the headend (or hub), the interface to the data-over-cable system is called the cable modem termination system-network-side interface (CMTS-NSI), and is specified in [15]. At customer locations, the interface is called the cable-modem-to-customer-premises-equipment interface (CMCI) and is specified in [14]. The intent is for operators to transfer IP traffic transparently between these interfaces.

The legal/regulatory classification of IP-based voice communications provided over cable networks and otherwise, and the legal/regulatory obligations, if any, borne by providers of such voice communications, are not yet fully defined by appropriate legal and regulatory authorities. Nothing in this specification is addressed to, or intended to affect, those issues. In particular, while this document uses standard terms such as “call,” “call signaling,” “telephony,” etc., it will be evident from this document that while a PacketCable network performs activities analogous to these PSTN functions, the manner by which it does so differs considerably from the manner in which they are performed in the PSTN by telecommunications carriers. These differences may be significant for legal/regulatory purposes.

2.2 Specification Goals

The goal of this specification document is to meet and to satisfy cable member companies (a.k.a. MSO), PacketCable, and CableLabs business and technical requirements.

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 PacketCable 1.0 MTA combined with a DOCSIS 1.1 Cable Modem. Both DOCSIS 1.1 and PacketCable 1.0 device provisioning steps MUST be performed for this embedded-MTA device to be provisioned. The embedded-MTA MUST have 2 IP addresses; an IP address for the CM component, and a different IP address for the MTA component. The embedded-MTA MUST have 2 MAC addresses, one MAC address for the CM component, and a different MAC address for the MTA-component.
- PacketCable 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. PacketCable makes no additional FQDN requirements on the CM component in the embedded-MTA beyond those required by DOCSIS 1.1. 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.
- PacketCable 1.0 embedded-MTA provisioning MUST support two separate configuration files, a DOCSIS-specified configuration file for the CM component, and a PacketCable-specified configuration file for the MTA component.
- PacketCable 1.0 allows one monolithic software image supporting both CM and MTA functionality to take advantage of the DOCSIS 1.1 software download mechanism. PacketCable 1.0 does not preclude vendor innovation to support separate software images for the CM and the MTA functionality.
- The embedded-MTA is outside the PacketCable network trust boundary as defined in the PacketCable architecture document [12].
- PacketCable 1.0 MUST support DOCSIS 1.1 software download as defined in [16].
- PacketCable 1.0 MUST support use of SNMPv3 security for network management operations.
- PacketCable 1.0 embedded-MTA provisioning minimizes the impact to DOCSIS 1.1 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 PacketCable 1.0 embedded-MTA provisioning.

- Where appropriate, the DOCSIS 1.1 management protocols are supported (SNMP, DHCP, TFTP).

2.3 PacketCable Reference Architecture

Figure 2 shows the reference architecture for the PacketCable 1.0 Network. Refer to the PacketCable Architecture Document [12] for more detailed information on this reference architecture.

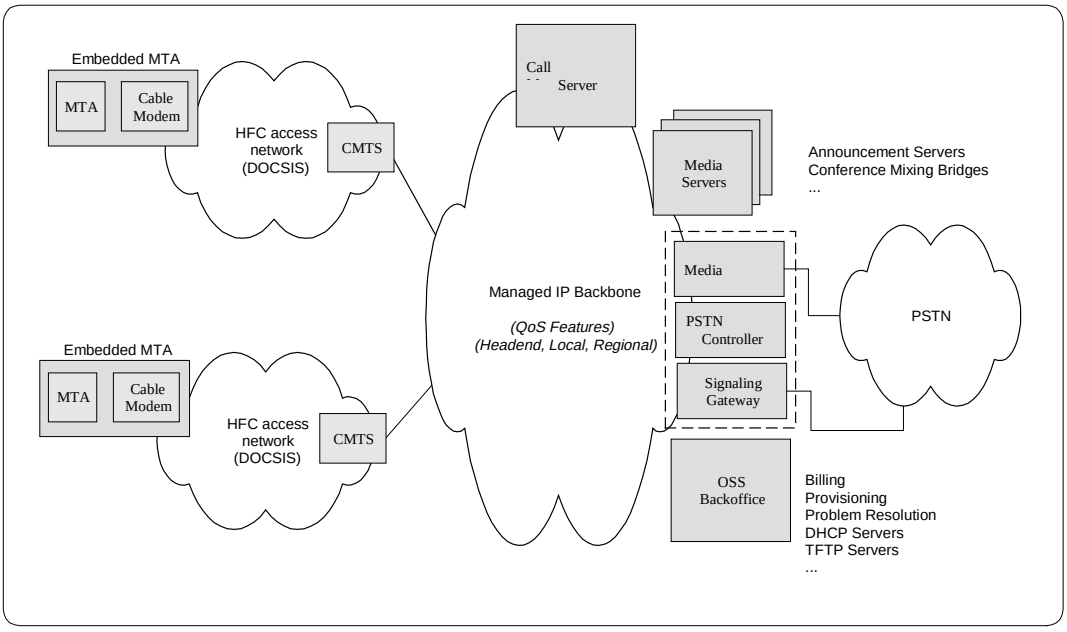


Figure 2: PacketCable 1.0 Network Component Reference Model (partial)

2.4 Components and Interfaces

The basic PacketCable 1.0 embedded-MTA provisioning reference architecture is shown in Figure 3. This figure represents the components and interfaces discussed in this document.

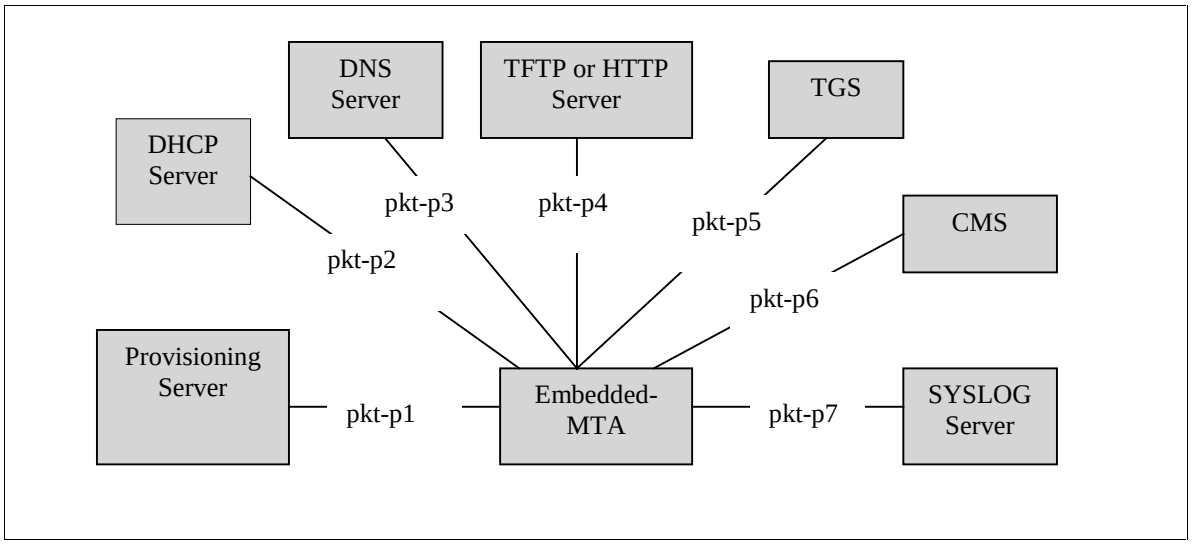


Figure 3: PacketCable Provisioning Interfaces

2.4.1 MTA

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

2.4.1.1 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 needs to obtain an MTA IP 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. Please refer to [12] for further information.
- The MTA needs to 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. This Service Provider Certificate is used as the key for verifying the MTA IP Telephony Certificate. Please refer to [12] for further information.

- 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 IP Telephony Certificate and the Service Provider Certificate.
- 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 [12].
- The MTA MUST establish a separate IPSEC security association with each CMS IP address in a CMS cluster [12].
- If the MTA already has an active security association with that CMS, the MTA MUST NOT request an additional Kerberos Ticket or new IPSEC security association with that CMS.

2.4.1.2 MTA SNMPv3 Requirements

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

- MTA SNMPv3 security is separate and distinct from DOCSIS 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 enrollment inform.
- SNMPv3 security will not be available until after successful processing of the configuration file.

2.4.2 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 includes a trap handler for provisioning enrollment and the provisioning status traps as well as a SNMP engine for retrieving device capabilities and setting the TFTP filename and access method. Refer to the PacketCable MTA MIB [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 PacketCable 1.0 and is left to vendor implementation. The interface between the Provisioning Server and the TFTP Server is not specified in PacketCable 1.0 and is left to vendor implementation.

2.4.3 Telephony Syslog Server

The PacketCable Telephony Syslog server functionally is identical to the DOCSIS 1.1 Syslog Server [21].

2.4.4 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 this 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.

2.4.5 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.

2.4.6 MTA to CMS

Signaling is the main interface between the MTA and the CMS. Refer to the PacketCable signaling document [11] for a detailed description of the interface.

- The CMS MUST accept signaling and bearer channel requests from a MTA that has an active security association.
- The CMS MUST NOT accept signaling and bearer channel requests from a MTA that does not have an active security association.

2.4.7 MTA to Security Server (TGS)

The interface between the MTA and the Ticket Granting Server (TGS) MUST conform to the PacketCable security specification [12].

2.4.8 MTA and Configuration Data File Access

This specification 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 a 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 a SNMPv3 SET from the provisioning server.

2.4.9 DOCSIS extensions for MTA Provisioning

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

- Additional values MUST be added to the DHCP option code 60 discover message.
- A new DHCP offer message option code 177 and the associated procedures MUST be implemented in DOCSIS.

3 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.

3.1 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 "611" service for in-band subscriber enrollment, or possibly "911" 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 a MTA device sealed object. Please refer to [12] for further information.

Please refer to section 2.4.1 for provisioning rules related to security associations.

3.2 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 signaling to be protected under the established security association.

Device registration will employ the Kerberos CMS Ticket the MTA obtained during subscriber enrollment. Please refer to [12] for further information.

3.3 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 the DOCSIS CM 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.

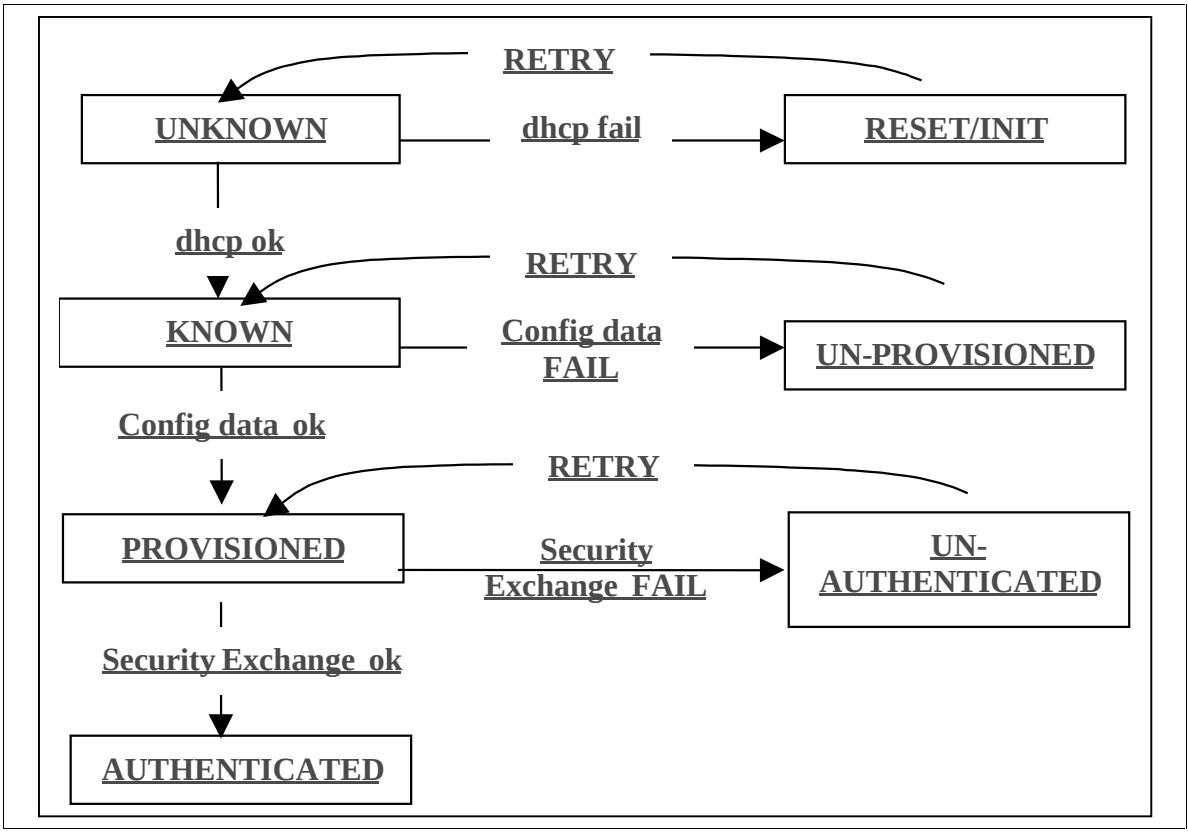


Figure 4. Device States and State Transitions

4 PROVISIONING FLOWS

4.1 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 behavior under mass-registration is beyond the scope of PacketCable 1.0, however this section provides the following recommendations and requirements.

- The recommendation for the throttling of registration MAY be based on DOCSIS 1.1 CM registration.
- The MTA MUST follow DHCP [1] and HTTP specification timeout and retry mechanisms.
- The MTA MUST use an adaptive timeout for TFTP as specified in the DOCSIS 1.1 specification.
- The MTA MUST follow backoff and retry recommendations that are defined in the security specification [12] for the security message flows.

4.2 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 a 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.

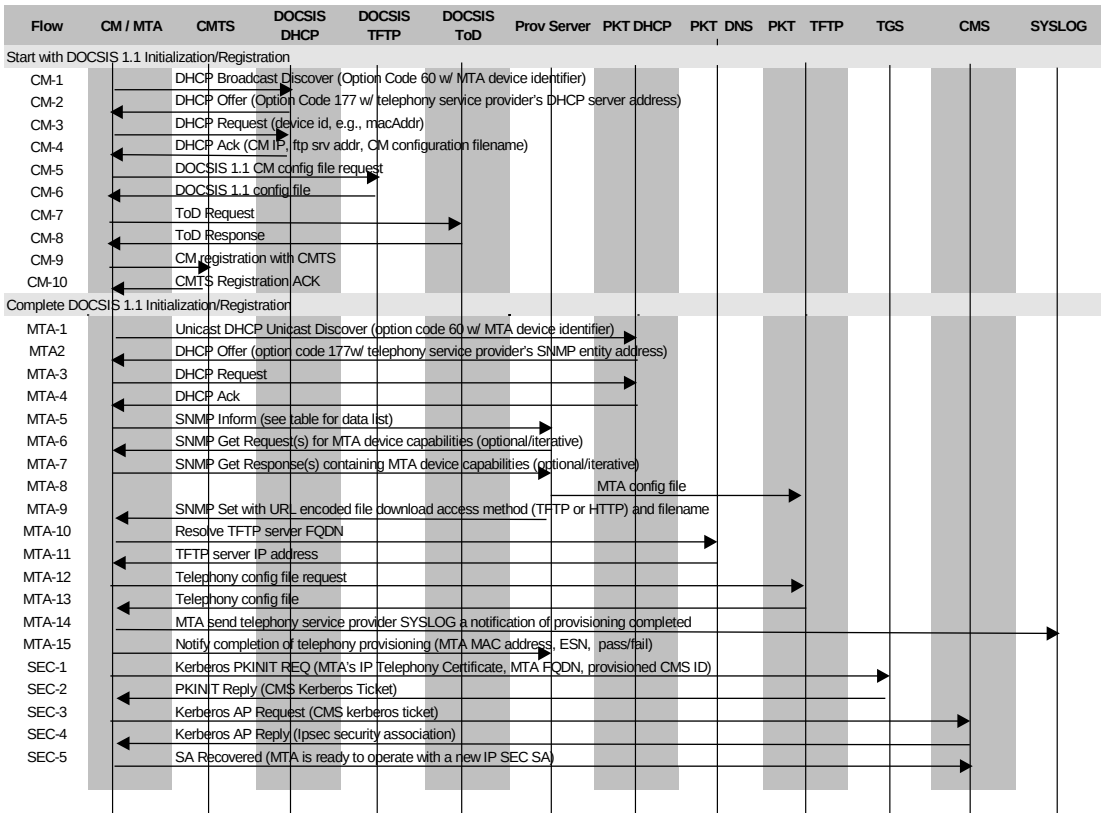


Figure 5. Embedded-MTA Power-on Initialization Flow

Flow	Embedded-MTA Power-On Initialization Flow Description	Proceed to here if this step fails
CM1	As defined in the DOCSIS 1.1 specified registration sequence, the client device begins device registration by having the cable modem 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 DOCSIS device or a DOCSIS device with an embedded MTA. The remainder of this message MUST conform to the DHCP discover data as defined in the DOCSIS 1.1 specification.	Per DOCSIS
CM2	One or more DHCP servers may respond with a DHCP offer message. To be considered a valid DHCP offer for PacketCable voice communications, the offer message MUST contain the PacketCable option code 177 with sub-option 1.	Per DOCSIS
CM3	The client device MUST select a single DHCP offer that includes the PacketCable code 177 values as defined in section 5.1 to function as a PacketCable voice communications-enabled device. The client device may select the first valid DHCP offer, or it may use it's 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 [1] in Appendix B for more details concerning the DHCP protocol.	Per DOCSIS
CM4	The DHCP server sends the client device cable modem component a DHCP ACK message to confirm acceptance of the offered data.	Per DOCSIS
CM5-CM10	The client device's cable modem component completes the remainder of the DOCSIS 1.1 specified registration sequence. This includes downloading the DOCSIS configuration file, requesting time of day registration, and registering with the CMTS.	Per DOCSIS
MTA1	The MTA sends a unicast DHCP DISCOVER message to the DHCP server address specified in the DOCSIS-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 DOCSIS device with an embedded MTA. (refer to section 5.2) .	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 PacketCable 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 MTA component sends the appropriate DHCP server a DHCP REQUEST message to accept the DHCP offer. Refer to [1] in Appendix B 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. Note: The FQDN MUST be available in the device before Kerberos Ticket generation can occur.	Per DHCP protocol
MTA5	The client device MTA component sends the PROV_SNMP_ENTITY a SNMPv3 INFORM requesting enrollment. The IP address of this PROV_SNMP_ENTITY is contained in the PacketCable DHCP offer message. As defined in the security spec [12], the MTA MUST create a randomly generated nonce and include the nonce in the MTA device signature. The following information MUST be in the "PktcMtaProvisioningEnrollment" object: • Hardware Version • Software Version • Device Identifier String (EMTA:PKTC1.0:DOCSIS1.1:xxxxxx) • MAC address • Telephony Provisioning Correlation ID • MTA device signature (includes randomly generated nonce value) This is used for authentication. Refer to the Security Spec [12] for more details. Please refer to the "PktcMtaProvisioningEnrollment" object in the MTA MIB [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. NOTE: 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 enrollment request. NOTE: Both the MTA device signature and the nonce MUST be regenerated every time this step occurs. NOTE: SNMPv3 initialization MUST have occurred prior to the sending of this inform.	MTA5

Flow	Embedded-MTA Power-On Initialization Flow Description	Proceed to here if this step fails
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 enrollment inform, with the exception of the SNMPv3 Get requests to get the MTA device certificate and MTA Manufacturer certificate. Refer to the security specification [12] 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 a 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>)" Note: 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	MTA9
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

Flow	Embedded-MTA Power-On Initialization Flow Description	Proceed to here if this step fails
MTA12	The MTA sends the TFTP Server a TFTP Get Request to request the specified configuration data file. Note: 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.	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 section 6.2 for MTA configuration file contents. NOTE: 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: SNMPv3 authentication and privacy keys are included in this configuration file. These keys are used to turn on PacketCable SNMPv3 security with both message integrity and privacy on all subsequent SNMP messages Enable SNMPv3 security if no error condition occurred during this step. If PacketCable and DOCSIS share the same SNMPv3 manager, then the SNMPv3 kickstart for DOCSIS MUST already have been enabled and MUST also have enabled SNMPv3 security for PacketCable and no additional PacketCable SNMPv3 security actions are required. Otherwise, SNMPv3 security for PacketCable 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 DOCSIS Cable Modem 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

Flow	Embedded-MTA Power-On Initialization Flow Description	Proceed to here if this step fails
	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. Note: SEC1 and SEC2 MUST be repeated for each CMS with which the MTA communicates.		
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. Note: SEC3, SEC4, and SEC5 MUST be repeated for each CMS with which the MTA communicates.		
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	
SEC5	(Required during error conditions – refer to security specification [12] 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	

4.3 Post Initialization Incremental Provisioning

This section 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)

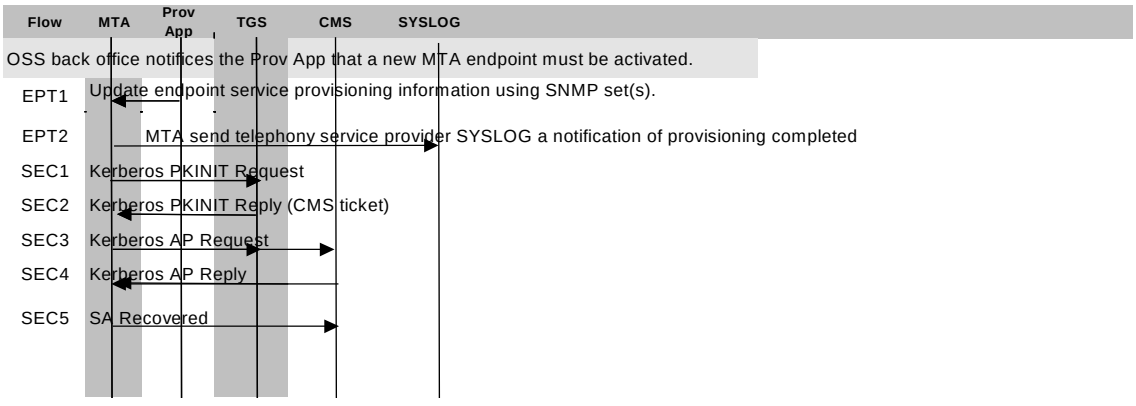
4.3.1 Synchronization of Provisioning Attributes with Configuration File

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 [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 this document, it is expected that, at a minimum, the following information is updated: customer records, and the MTA configuration file on the TFTP or HTTP server.

4.3.2 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).

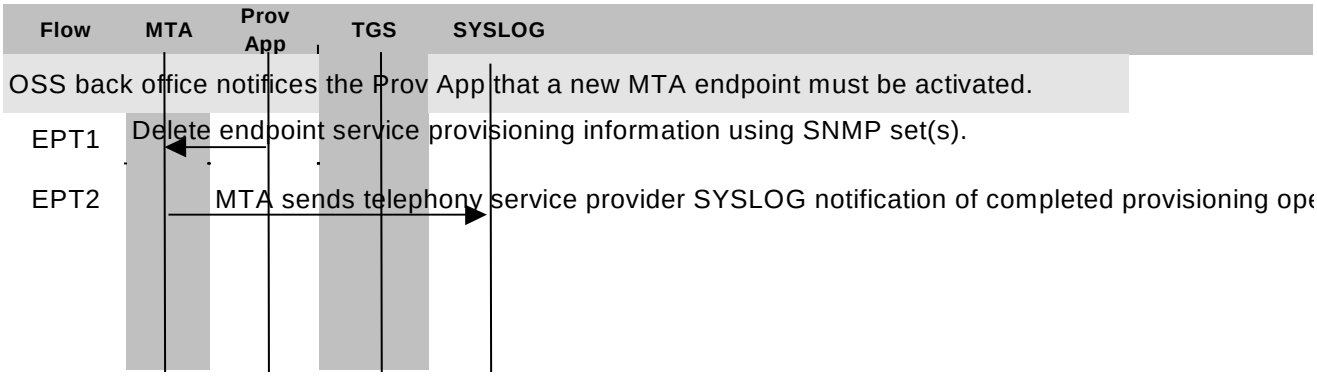
MTA Endpoint services are enabled using SMNPv3 via the MTA MIB [8]. In this example, a subscriber is requesting that additional service be added. This example assumes the service provider's account creation process has been completed, and shows only the applications critical for the flows. For instance,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



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 section 2.4.1 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 DOCSIS Cable Modem 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 IP 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 [12] 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

4.3.3 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.



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 DOCSIS Cable Modem Device MIB specification details on SYSLOG events.

4.3.4 Modifying Services on an MTA Endpoint

MTA Endpoint services are modified using SMNPv3 Sets to the MTA MIB [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 DOCSIS 1.1 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.

4.4 MTA Replacement

The initialization sequence for the replaced MTA will be same as the MTA's first-time initialization described in section 4. 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 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 this document.

The initialization flow as described in section 4 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.

4.5 Temporary Signal Loss

The treatment for RF loss in the MTA MUST be similar to that of a DOCSIS 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 section 4.

5 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. These DHCP options are currently defined in a draft proposal submitted to the Internet Engineering Task Force (IETF) DHCP committee [10].

5.1 Code 177: PacketCable Servers Option

DHCP option code 177 is a temporary code that the PacketCable embedded-MTA device can use until a permanent code is assigned by the IETF. Refer to the power-on initialization flows in section 4 for further details.

DHCP option code 177 is used in both the CM and MTA DHCP OFFER messages to identify a list of valid PacketCable network servers. The PacketCable servers are identified using either an IPv4 address or a FQDN. Each sub-option of DHCP option code 177 identifies a particular type of PacketCable server. Sub-option 1 identifies the PacketCable network DHCP server, sub-option 2 identifies the PacketCable service provider's SNMP entity, and sub-options 3 and 4 identifies the primary and secondary PacketCable network DNS servers. Refer to RFC 2132 section 2 [2] for DHCP encoding and formatting details.

During the DOCSIS 1.1 device provisioning sequence of an embedded-MTA, the following fields MUST be included in the CM's DHCP OFFER message. PacketCable-defined DHCP option fields are encoded in the following format using option code 177.

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

The following sections provide detailed descriptions of each sub-option of DHCP option code 177. Note that UDP port numbers are normally standard values as defined in [3]. 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 [3] is assumed. For example, the standard DNS UDP port number is 42/udp.

5.1.1 Service Provider's DHCP Server Address (sub-option 1)

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.

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 format 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 1 is as follows:

Option	Sub-option	Value	Comments
177	1	[xxx.xxx.xxx.xxx]:NNNN	Either the IP address or the FQDN will be configured. Where NNNN is an optional UDP port number if different than the well-known port defined in [3].
		FQDN:NNNN	

5.1.2 Service Provider's SNMP Entity Address (sub-option 2)

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 2 is as follows:

Option	Sub-option	Value	Comments
177	2	[xxx.xxx.xxx.xxx]:NNNN	Either the IPv4 address or the FQDN will be configured. Where NNNN is an optional UDP port number if different than the well-known port defined in [3].
		FQDN:NNNN	

5.1.3 DNS system (sub-option 3 and sub-option 4)

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

Sub-option 3 is the address of the network's primary DNS server and MUST be specified if sub-option 1 or sub-option 2 is in FQDN format. Sub-option 4 is the address of the network's secondary DNS server. Sub-option 4 MAY be specified to identify a redundant or backup DNS server.

The encoding syntax for sub-option 3 and sub-option 4 is as follows:

Option	Sub-option	Value	Comments
177	3	[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 than the well-known port defined in [3].
177	4	[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 than the well known port defined in [3].

5.2 Code 60: Vendor Client Identifier

Option code 60 contains encoded ASCII values representing the type of PacketCable MTA. Possible values are for an embedded MTA and for future use a standalone 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 PacketCable extensions to the DOCSIS 1.1 option 60 requirements.

Option	Length	Value	Comments
60	30	EMTA:PKTC1.0:DOCSIS1.1:xxx xxxx	The CM-component and the MTA-component encodes option 60 in the DHCP messages. Where PKTC stands for PacketCable, and EMTA, refers to embedded MTA and SMTA refers to Standalone MTA. The suffix xxxxxxx are defined by DOCSIS 1.1.
		EMTA:PKTC1.1:DOCSIS1.1:xxx xxxx	
		SMTA:PKTC1.0:DOCSIS1.1:xxx xxxx (for future use)	
		SMTA:PKTC1.1:DOCSIS1.1:xxx xxxx (for future use)	

6 MTA PROVISIONABLE ATTRIBUTES

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

PacketCable 1.0 requires that a 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 section 6.2.1.

6.1 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.

6.2 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 "type length and value" (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 DOCSIS TLV type 11.

Type	Length	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 MTA configuration file MUST start with the "telephony configuration file start" tag and MUST end with the "telephony configuration file end" tag. These tags enable the MTA TLV parameters to be distinguished from DOCSIS TLV parameters. 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 enrollment 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 section 4.3.1 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 section 4.3.1 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.

6.2.1 Device Level Configuration Data

Refer to the MTA MIB [8] for more detailed information concerning these attributes and their default values.

- The MTA Device signature is sent by the MTA to authenticate messages it sends to other servers in MTA-5 and MTA-7. There is no privacy of capability data unless enabled in SNMPv3 prior to flow MTA-5
- The MTA Manufacturer Certificate validates the MTA Device Certificate.

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.

Attribute	Syntax	Configuration Access	SNMP Access	Comments
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.
Packet Cable MTA Device FQDN	String	W, required (refer to note)	R/W	Fully Qualified Domain Name for this Device. **Note**: 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.
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 DOCSIS 1.1 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 DOCSIS 1.1 DHCP offer MUST be used.

Attribute	Syntax	Configuration Access	SNMP Access	Comments
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 NULL in the MTA config file, then the address of the syslog server provided in the DOCSIS CableDevice MIB MUST be used. If this value is 0.0.0.0, then it implies that syslog logging for the MTA is turned off.
PacketCable Telephony Provisioning Correlation ID	Interger32	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 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. 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. Note: This object is a MIB table index.
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.

Attribute	Syntax	Configuration Access	SNMP Access	Comments
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.

6.2.2 Device Level Service Data

Refer to the MTA MIB [8], the NCS MIB [9], the NCS Call Signaling specification [11] and RFC 2475 [28] for more detailed information concerning these attributes and their default values.

Attribute	Syntax	Configuration Access	SNMP Access	Comments
NCS Default Call Signaling TOS	Integer	W, required	R/W	The default value used in the IP header for setting the TOS value for NCS call signaling.
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 signaling and media TOS values. Allowed values are "IPv4 TOS octet" or "DSCP codepoint". Refer to IETF RFC 2475.
R0 cadence	Bit-field	W,required	R/W	User defined bit field where each bit represents a duration of 200 milliseconds (6 seconds 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 milliseconds (6 seconds 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 milliseconds (6 seconds total) 1 = active ringing, 0 = silence If this field is not going to be used, it MUST be set to zero.

6.2.3 Per-Endpoint Configuration Data

Refer to the NCS MIB [9], the NCS spec [11], the security spec [12] and the MTA MIB [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 2 different endpoints share the same CMS FQDN then all 6 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 2 different endpoints share the same Kerberos Realm and same CMS Kerberos Principal Name, then these 4 attributes MUST be identical: PKINIT grace period, TGS name list, MTA IP telephony certificate, telephony service provider certificate.

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 prt 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 CMS's 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

Attribute	Syntax	Access	SNMP Access	Comments
				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.
Telephony Service Provider Certificate	String	W,required	R/W	The Telephony Service Provider's X.509 public-key certificate given to all MTA's who have signed up with the given Telephony Service Provider.
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. NOTE: If this certificate contains the MTA's IPv4 address, then any time the IPv4

Attribute	Syntax	Access	SNMP Access	Comments
				address changes, the Telephony Service Provider MUST issue the MTA a new certificate.
Call Management Server Kerberos Principal Name	String	W, required	R/W	Identifies a collection of CMS's 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 2 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.

7 MTA DEVICE CAPABILITIES

MTA device capabilities information is contained in a combination of MIBs including: IETF's MIB-II, the MTA MIB [8] the NCS MIB [9] and the DOCSIS 1.1 CableDevice MIB. Use of capabilities information by the Provisioning Application is optional. Examples of capabilities information includes:

Attribute
HTTP Download FileAccess 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

Appendix A. Acknowledgements

On behalf of CableLabs and its participating member companies, I would like to extend a heartfelt thanks to all those who contributed to the development of this specification. Certainly all the participants of the provisioning focus team have added value to this effort by participating in the review and weekly conference calls. Particular thanks are given to Burcak Besar (3Com); Angela Lyda, Rick Morris (Arris Interactive); Steven Bellovin (AT&T); Jiri Matousek (Bay Networks); Klaus Hermanns, Azita Kia, Michael Thomas, Rich Woundy (Cisco); Deepak Patil (Com21); Jeff Ollis, Rick Vetter (General Instrument); Roger Loots (Lucent); Roy Spitzer (Telogy), Aviv Goren (Terayon); and Prithivraj Narayanan (Wipro). A special thanks is due Rick Morris (Arris), Sasha Medvinsky (GI), and Raj Deshpande (Motorola) who worked tirelessly in a challenging multi-vendor environment to build this specification.

Maria Stachelek and Frank Christofferson, CableLabs

Appendix B. References and Bibliography

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

[2]. DHCP Options and BOOTP Vendor Extensions, IETF, RFC 2132, March 1997.

[3]. ASSIGNED NUMBERS, IETF (contains ARP/DHCP parameters), RFC 1340, July 1992.

[4]. The TFTP Protocol (Revision 2), STD 33, RFC 1350, MIT, July 1992.

[5]. Domain Names—Concepts and Facilities, IETF, RFC 1034, STD 13, November 1987.

[6]. Domain Names—Implementation and Specifications, IETF RFC 1035, November 1987.

[7]. Domain Name System Structure and Delegation, IETF, RFC 1591, March 1994.

[8]. "PacketCable MTA MIB," PKT-SP-MIBS-MTA-I01-991201, Cable Television Laboratories, Inc., December 1, 1999. http://www.PacketCable.com./

[9]. "PacketCable NCS MIB," PKT-SP-MIBS-NCS-I01-991201, Cable Television Laboratories, Inc., December 1, 1999. http://www.PacketCable.com./

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

[11]. "PacketCable Network-Based Call Signaling Protocol Specification**,"** PKT-SP-EC-MGCP-I02-991201, Cable Television Laboratories, Inc., December 1, 1999, http://www.PacketCable.com./

[12]. "PacketCable Security Specification," PKT-SP-SEC-I01-991201, Cable Television Laboratories, Inc., December 1, 1999, http://www.PacketCable.com./

[13]. PacketCable Architecture Framework Technical Report, PKT-TR-ARCH-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., December 1, 1999, http://www.PacketCable.com./

[14]. Cable Modem to Customer Premise Equipment Interface Specification, CMCI, DOCSIS SP-CMCI-I02-980317, Cable Television Laboratories, Inc.

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

[16]. "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/

[17]. SNMPv2-TM, RFC1449.

[18]. SNMPv2-TC, RFC1903.

[19]. "PacketCable Audio/Video Codecs Specification," PKT-SP-CODEC-I01-991201, December 1, 1999, Cable Television Laboratories, Inc., http://www.PacketCable.com./

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

[21]. **"**PacketCable Dynamic Quality of Service Specification**,"** PKT-SP-DQOS-I01-991201, Cable Television Laboratories, Inc., December 1, 1999, http://www.PacketCable.com./

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

[23]. SIMPLE MAIL TRANSFER PROTOCOL, IETF RFC-821, August 1982.

[24]. A Simple Network Management Protocol (SNMP), IETF RFC-1157, May 1990.

[25]. Braden, R., Requirements for Internet Hosts -- Application and Support, IETF RFC-1123, October 1989.

[26]. TFTP Timeout Interval and Transfer Size Options, IETF RFC-2349, May 1998.

[27]. HTTP, IETF RFC1945, IETF RFC2068.

[28]. An Architecture for Differentiated Services, IETF RFC-2475, December 1998

Appendix C. Glossary

AAA	Authentication, Authorization and Accounting
Access Control	Limiting the flow of information from the resources of a system only to authorized persons, programs, processes or other system resources on a network.
Active	A service flow is said to be "active" when it is permitted to forward data packets. A service flow must first be admitted before it is active.
Admitted	A service flow is said to be "admitted" when the CMTS has reserved resources (e.g. bandwidth) for it on the DOCSIS network.
AF	Assured Forwarding. A Diffserv Per Hop Behavior.
AH	Authentication header is an IPSec security protocol that provides message integrity for complete IP packets, including the IP header.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access".
Announcement Server	An announcement server plays informational announcements in PacketCable network. Announcements are needed for communications that do not complete and to provide enhanced information services to the user.
AMA	Automated Message Accounting., a standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies)
Asymmetric Key	An encryption key or a decryption key used in a public key cryptography, where encryption and decryption keys are always distinct.
AT	Access Tandem
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
Authentication	The process of verifying the claimed identity of an entity to another entity.
Authenticity	The ability to ensure that the given information is without modification or forgery and was in fact produced by the entity who claims to have given the information.
Authorization	The act of giving access to a service or device if one has the permission to have the access.
BAF	Bellcore AMA Format, another way of saying AMA
BPI+	Baseline Privacy Interface Plus is the security portion of the DOCSIS 1.1 standard which runs on the MAC layer.
CBC	Cipher block chaining mode is an option in block ciphers that combine (XOR) the previous block of ciphertext with the current block of plaintext before encrypting that block of the message.
CBR	Constant Bit Rate.
CA	Certification Authority - a trusted organization that accepts certificate applications from entities, authenticates applications, issues certificates and maintains status information about certificates.
CA	Call Agent. In this specification "Call Agent" is part of the CMS that maintains the communication state, and controls the line side of the communication.

CDR	Call Detail Record. A single CDR is generated at the end of each billable activity. A single billable activity may also generate multiple CDRs
CIC	Circuit Identification Code. In ANSI SS7, a two octet number that uniquely identifies a DSO circuit within the scope of a single SS7 Point Code.
CID	Circuit ID (Pronounced "Kid"). This uniquely identifies an ISUP DS0 circuit on a Media Gateway. It is a combination of the circuit's SS7 gateway point code and Circuit Identification Code (CIC). The SS7 DPC is associated with the Signaling Gateway that has domain over the circuit in question.
CIF	Common Intermediate Format
Cipher	An algorithm that transforms data between plaintext and ciphertext.
Ciphersuite	A set which must contain both an encryption algorithm and a message authentication algorithm (e.g. a MAC or an HMAC). In general, it may also contain a key management algorithm, which does not apply in the context of PacketCable.
Ciphertext	The (encrypted) message output from a cryptographic algorithm that is in a format that is unintelligible.
CIR	Committed Information Rate.
Cleartext	The original (unencrypted) state of a message or data.
CM	DOCSIS Cable Modem.
CMS	Cryptographic Message Syntax
CMS	Call Management Server. Controls the audio connections. Also called a Call Agent in MGCP/SGCP terminology.
CMTS	Cable Modem Termination System, the device at a cable head-end which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
Codec	COder-DECoder
Confidentiality	A way to ensure that information is not disclosed to any one other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
COPS	Common Open Policy Service Protocol is currently an internet draft which describes a client/server model for supporting policy control over QoS Signaling Protocols and provisioned QoS resource management.
CoS	Class of Service. The type 4 tuple of a DOCSIS 1.0 configuration file.
CSR	Customer Service Representative
Cryptoanalysis	The process of recovering the plaintext of a message or the encryption key without access to the key.
Cryptographic algorithm	An algorithm used to transfer text between plaintext and ciphertext.
DA	Directory Assistance
DE	Default. A Diffserv Per Hop Behavior.
Decipherment	A procedure applied to ciphertext to translate it into plaintext.
Decryption	A procedure applied to ciphertext to translate it into plaintext.
Decryption key	The key in the cryptographic algorithm to translate the ciphertext to plaintext
DHCP	Dynamic Host Configuration Protocol.
DHCP-D	DHCP Default - Network Provider DHCP Server

Digital certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a public key certificate
Digital signature	A data value generated by a public key algorithm based on the contents of a block of data and a private key, yielding an individualized cryptographic checksum
DNS	Domain Name Server
Downstream	The direction from the head-end toward the subscriber location.
DSCP	Diffserv Code Point. A field in every IP packet which identifies the Diffserv Per Hop Behavior. In IP version 4, the TOS byte is redefined to be the DSCP. In IP version 6, the Traffic Class octet is used as the DSCP. See Appendix A.
DOCSIS	Data Over Cable System Interface Specification.
DPC	Destination Point Code. In ANSI SS7, a 3 octet number which uniquely identifies an SS7 Signaling Point, either an SSP, STP, or SCP.
DQoS	Dynamic Quality of Service, i.e. assigned on the fly for each communication depending on the QoS requested
DTMF	Dual-tone Multi Frequency (tones)
EF	Expedited Forwarding. A Diffserv Per Hop Behavior.
E-MTA	Embedded MTA – a single node which contains both an MTA and a cable modem.
Encipherment	A method used to translate information in plaintext into ciphertext.
Encryption	A method used to translate information in plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or MCU
EO	End Office
Errored Second	Any 1-sec interval containing at least one bit error.
ESP	IPSec Encapsulation Security Payload protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute
Event Message	Message capturing a single portion of a connection
FGD	Feature Group D signaling
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated"
Flow [IP Flow]	A unidirectional sequence of packets identified by ISO Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Flow [DOCSIS Flow]	(a.k.a. DOCSIS-QoS "service flow"). A unidirectional sequence of packets associated with a SID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow.
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 821 for details.
Gateway	Devices bridging between the PacketCable IP Voice Communication world and the PSTN. Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signaling Gateway which sends and receives circuit switched network signaling tot he edge of the PacketCable network.

H.323	An ISO standard for transmitting and controlling audio and video information. The H.323 standard requires the use of the H.225/H.245 protocol for communication control between a "gateway" audio/video endpoint and a "gatekeeper" function.
Header	Protocol control information located at the beginning of a protocol data unit.
HFC	Hybrid Fiber/Coax(ial [cable]), HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the head-end and the fiber nodes, and coaxial distribution from the fiber nodes to the customer locations.
H.GCP	A protocol for media gateway control being developed by ITU.
HMAC	Hashed Message Authentication Code – a message authentication algorithm, based on either SHA-1 or MD5 hash and defined in RFC 2104.
HTTP	Hyper Text Transfer Protocol. Refer to IETF RFC 1945 and RFC 2068.
IANA	Internet Assigned Numbered Authority. See www.ietf.org for details.
IC	Inter-exchange Carrier
IETF	Internet Engineering Task Force. A body responsible, among other things, for developing standards used in the Internet.
IKE	Internet Key Exchange is a key management mechanism used to negotiate and derive keys for SAs in IPSec.
IKE–	A notation defined to refer to the use of IKE with pre-shared keys for authentication.
IKE+	A notation defined to refer to the use of IKE, which requires digital certificates for authentication.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access Transport Area
IP	Internet Protocol. An Internet network-layer protocol.
IPSec	Internet Protocol Security, a collection of Internet standards for protecting IP packets with encryption and authentication.
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part is a protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ISTP	Internet Signaling Transport Protocol
ISTP – User	Any element, node, or software process that uses the ISTP stack for signaling communications.
ITU	International Telecommunication Union
IVR	Interactive Voice Response System
Jitter	Variability in the delay of a stream of incoming packets making up a flow such as a voice communication.
Kerberos	A secret-key network authentication protocol that uses a choice of cryptographic algorithms for encryption and a centralized key database for authentication.
Key	A mathematical value input into the selected cryptographic algorithm.
Key Exchange	The swapping of public keys between entities to be used to encrypt communication between the entities.

Key Management	The process of distributing shared symmetric keys needed to run a security protocol.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Key Pair	An associated public and private key where the correspondence between the two are mathematically related, but it is computationally infeasible to derive the private key from the public key.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
LATA	Local Access and Transport Area
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
LD	Long Distance
LIDB	Line Information Data Base, containing information on customers required for real-time access such as calling card personal identification numbers (PINs) for real-time validation
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
LLC	Logical Link Control, used here to mean the Ethernet Packet header and optional 802.1P tag which may encapsulate an IP packet. A sublayer of the Data Link Layer.
LNP	Local Number Portability. Allows a customer to retain the same number when switching from one local service provider to another.
LSSGR	LATA Switching Systems Generic Requirements
MAC	Message Authentication Code - a fixed length data item that is sent together with a message to ensure integrity, also known as a MIC.
MAC	Media Access Control. It is a sublayer of the Data Link Layer. It normally runs directly over the physical layer.
MC	Multipoint Controller
MD5	Message Digest 5 - a one-way hash algorithm which maps variable length plaintext into fixed length (16 byte) ciphertext.
MDCP	A media gateway control specification submitted to IETF by Lucent. Now called SCTP.
MDU	Multi-Dwelling Unit. Multiple units within the same physical building. The term is usually associated with high rise buildings
MEGACO	Media Gateway Control IETF working group. See www.ietf.org for details.
MG	The media gateway provides the bearer circuit interfaces to the PSTN and transcodes the media stream.
MGC	An Media Gateway Controller is the overall controller function of the PSTN gateway. It receives, controls and mediates call signaling information between the PacketCable and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow on to SGCP.
MIB	Management Information Base
MIC	Message integrity code, a fixed length data item that is sent together with a message to ensure integrity, also known as a MAC.
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media

	streams of multiple connections.
MSO	Multi-System Operator, a cable company that operates many head-end locations in several cities.
MSU	Message Signal Unit
MTA	Media Terminal Adapter – contains the interface to a physical voice device, a network interface, CODECs, and all signaling and encapsulation functions required for VoIP transport, class features signaling, and QoS signaling.
MTP	The Message Transfer Part is a set of two protocols (MTP 2, 3) within the SS7 suite of protocols that are used to implement physical, data link and network level transport facilities within an SS7 network.
MWD	Maximum Waiting Delay
NANP	North American Numbering Plan
NANPNAT	North American Numbering Plan Network Address Translation
NAT Network Layer	Network Address Translation Layer 3 in the Open System Interconnection (OSI) architecture; the layer that provides services to establish a path between open systems.
Network Layer	Layer 3 in the Open System Interconnection (OSI) architecture that provides network information that is independent from the lower layers.
Network Management	The functions related to the management of data across the network.
Network Management OSS	The functions related to the management of data link layer and physical layer resources and their stations across the data network supported by the hybrid fiber/coax system.
NCS	Network Call Signaling
Nonce	A random value used only once which is sent in a communications protocol exchange to prevent replay attacks.
Non-Repudiation	The ability to prevent a sender from denying later that he or she sent a message or performed an action.
NPA-NXX	Numbering Plan Area (more commonly known as area code) NXX (sometimes called exchange) represents the next three numbers of a traditional phone number. The N can be any number from 2-9 and the Xs can be any number. The combination of a phone number's NPA-NXX will usually indicate the physical location of the call device. The exceptions include toll-free numbers and ported number (see LNP)
NTP	Network Time Protocol, an internet standard used for synchronizing clocks of elements distributed on an IP network
NTSC	National Television Standards Committee which defines the analog color television, broadcast standard used today in North America.
Off-Net Call	A communication connecting a PacketCable subscriber out to a user on the PSTN
On-Net Call	A communication placed by one customer to another customer entirely on the PacketCable Network
One-way Hash	A hash function that has an insignificant number of collisions upon output.
OSP	Operator Service Provider
OSS-D	OSS Default – Network Provider Provisioning Server
OSS	Operations Systems Support. The back office software used for configuration, performance, fault, accounting and security management.

PAL	Phase Alternate Line – the European color television format which evolved from the American NTSC standard.
PDU	Protocol Data Unit
PKCS	Public Key Cryptography Standards, published by RSA Data Security Inc. Describes how to use public key cryptography in a reliable, secure and interoperable way.
PKI	Public Key Infrastructure - a process for issuing public key certificates, which includes standards, Certification Authorities, communication between authorities and protocols for managing certification processes.
PKINIT	The extension to the Kerberos protocol that provides a method for using public key cryptography during initial authentication.
PHS	Payload Header Suppression, a DOCSIS technique for compressing the Ethernet, IP and UDP headers of RTP packets.
Plaintext	The original (unencrypted) state of a message or data.
Pre-shared Key	A shared secret key passed to both parties in a communication flow, using an unspecified manual or out-of-band mechanism.
Privacy	A way to ensure that information is not disclosed to any one other then the intended parties. Information is usually encrypted to provide confidentiality. Also known as confidentiality.
Private Key	The key used in public key cryptography that belongs to an individual entity and must be kept secret.
Proxy	A facility that indirectly provides some service or acts as a representative in delivering information there by eliminating a host from having to support the services themselves.
PSC	Payload Service Class Table, a MIB table that maps RTP payload Type to a Service Class Name.
PSFR	Provisioned Service Flow Reference. An SFR that appears in the DOCSIS configuration file.
PSTN	Public Switched Telephone Network.
Public Key	The key used in public key cryptography that belongs to an individual entity and is distributed publicly. Other entities use this key to encrypt data to be sent to the owner of the key.
Public Key Certificate	A binding between an entity's public key and one or more attributes relating to its identity, also known as a digital certificate.
Public Key Cryptography	A procedure that uses a pair of keys, a public key and a private key for encryption and decryption, also known as asymmetric algorithm. A user's public key is publicly available for others to use to send a message to the owner of the key. A users private key is kept secret and is the only key which can decrypt messages sent encrypted by the users public key.
PCM	Pulse Code Modulation – A commonly employed algorithm to digitize an analog signal (such as a human voice) into a digital bit stream using simple analog to digital conversion techniques.
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service, guarantees network bandwidth and availability for applications.
RADIUS	Remote Access Dial-In User Service, an internet protocol (RFC 2138 and RFC 2139) originally designed for allowing users dial-in access to the internet through remote servers. Its flexible design has allowed it to be extended well

	beyond its original intended use
RAS	Registration, Admissions and Status. RAS Channel is an unreliable channel used to convey the RAS messages and bandwidth changes between two H.323 entities.
RC4	A variable key length stream cipher offered in the ciphersuite, used to encrypt the media traffic in PacketCable.
RFC	Request for Comments. Technical policy documents approved by the IETF which are available on the World Wide Web at http://www.ietf.cnri.reston.va.us/rfc.html
RFI	The DOCSIS Radio Frequency Interface specification.
RJ-11	Standard 4-pin modular connector commonly used in the United States for connecting a phone unit into the wall jack
RKS	Record Keeping Server, the device which collects and correlates the various Event Messages
Root Private Key	The private signing key of the highest level Certification Authority. It is normally used to sign public key certificates for lower-level Certification Authorities or other entities.
Root Public Key	The public key of the highest level Certification Authority, normally used to verify digital signatures that it generated with the corresponding root private key.
RSA Key Pair	A public/private key pair created for use with the RSA cryptographic algorithm.
RSVP	Resource reSerVation Protocol
RTCP	Real Time Control Protocol
RTO	Retransmission Timeout
RTP	Real Time Protocol, a protocol defined in RFC 1889 for encapsulating encoded voice and video streams.
S-MTA	Standalone MTA – a single node which contains an MTA and a non DOCSIS MAC (e.g. ethernet).
SA	Security Association - a one-way relationship between sender and receiver offering security services on the communication flow .
SAID	Security Association Identifier - uniquely identifies SAs in the BPI+ security protocol, part of the DOCSIS 1.1 specification.
SCCP	The Signaling Connection Control Part is a protocol within the SS7 suite of protocols that provides two functions in addition to those that are provided within MTP. The first is the ability to address applications within a signaling point. The second function is Global Title Translation.
SCP	A Service Control Point is a Signaling Point within the SS7 network, identifiable by a Destination Point Code, that provides database services to the network.
SCTP	Simple Control Transmission Protocol.
SDP	Session Description Protocol.
SDU	Service Data Unit. Information that is delivered as a unit between peer service access points.
Secret Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a symmetric key.

Session Key	A cryptographic key intended to encrypt data for a limited period of time, typically between a pair of entities.
SF	Service Flow. A unidirectional flow of packets on the RF interface of a DOCSIS system.
SFID	Service Flow ID, a 32-bit integer assigned by the CMTS to each DOCSIS Service Flow defined within a DOCSIS RF MAC domain. Any 32-bit SFID must not conflict with a zero-extended 14-bit SID. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). USFIDs and DSFIDs are allocated from the same SFID number space.
SFR	Service Flow Reference, a 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
SG	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1 - a one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed by using encryption.
SIP	Session Initiation Protocol is an application layer control (signaling) protocol for creating, modifying and terminating sessions with one or more participants.
SIP+	Session Initiation Protocol Plus is an extension to SIP.
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SPI	Security Parameters Index - a field in the IPSEC header that along with the destination IP address provides a unique number for each SA.
SS7	Signaling System Number 7. SS7 is an architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Signal Switching Point. SSPs are points within the SS7 network that terminate SS7 signaling links and also originate, terminate, or tandem switch calls.
STP	Signal Transfer Point. An STP is a node within an SS7 network that routes signaling messages based on their destination address. It is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and source and destination UDP/TCP port.
Symmetric Key	The cryptographic key used in a symmetric key algorithm, which results in the secrecy of the encrypted data depending solely upon keeping the key a secret, also known as a secret key.
Systems Management	Functions in the application layer related to the management of various open systems Interconnection (OSI) resources and their status across all layers of the OSI architecture.

TCAP	Transaction Capabilities Application Protocol. A protocol within the SS7 stack that is used for performing remote database transactions with a Signaling Control Point.
TCP	Transmission Control Protocol
TD	Timeout for Disconnect
TFTP	Trivial File Transfer Protocol
TFTP-D	Default – Trivial File Transfer Protocol
TGS	Ticket Granting Server used to grant Kerberos tickets.
TGW	Telephony Gateway
TIPHON	Telecommunications & Internet Protocol Harmonization Over Network.
TLV	Type-Length-Value tuple within a DOCSIS configuration file.
TN	Telephone Number
ToD	Time of Day Server
TOS	Type of Service. An 8-bit field of every IP version 4 packet. In a Diffserv domain, the TOS byte is treated as the Diffserv Code Point, or DSCP.
Transit Delays	The time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.
Trunk	An analog or digital connection from a circuit switch which carries user media content and may carry voice signaling (MF, R2, etc.).
TSG	Trunk Subgroup
Tunnel Mode	An IPSEC (ESP or AH) mode that is applied to an IP tunnel, where an outer IP packet header (of an intermediate destination) is added on top of the original, inner IP header. In this case, the ESP or AH transform treats the inner IP header as if it were part of the packet payload. When the packet reaches the intermediate destination, the tunnel terminates and both the outer IP packet header and the IPSEC ESP or AH transform are taken out.
UDP	User Datagram Protocol, a connectionless protocol built upon Internet Protocol (IP).
Upstream	The direction from the subscriber location toward the head-end.
VAD	Voice Activity Detection
VBR	Variable bit-rate
VoIP	Voice over IP
WBEM	Web-Based Enterprise Management (WBEM) is the umbrella under which the DMTF (Desktop Management Task Force) will fit its current and future specifications. The goal of the WBEM initiative is to further management standards using Internet technology in a manner that provides for interoperable management of the Enterprise. There is one DMTF standard today within WBEM and that is CIM (Common Information Model). WBEM compliance means adhering to the CIM. See www.dmtf.org
X.509 certificate	a public key certificate specification developed as part of the ITU-T X.500 standards directory

Appendix D. Revisions

Engineering Change Numbers

ECN	Date Ratified	Summary