PacketCable™ MTA Device Provisioning Specification

PKT-SP-PROV-I04-021018

ISSUED

Notice

Document Status Sheet

Document Control Number:	PKT-SP-PROV-I04-021018			
Document Title:	PacketCable™ MTA Device Provisioning Specification			
Revision History:	I01 – Released December 01, 1999 I02 – Released March 23, 2001 I03 – Released December 21, 2001 I04 – Released October 18, 2002			
Date:	October 18, 2002			
Status:	~~Work in Progress~~	~~Draft~~	Issued	~~Closed~~
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.
Issued	A stable document, which has undergone rigorous member and vendor review and is suitable for product design and development, cross-vendor interoperability, and for certification testing.
Closed	A static document, reviewed, tested, validated, and closed to further engineering change requests to the specification through CableLabs.

Contents

Figures

1 INTRODUCTION

1.1 Purpose

This specification describes the PacketCable™ 1.0 embedded-MTA device initialization and provisioning. This specification is issued to facilitate design and field-testing leading to the early manufacturability 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 – References
- Section 3 – Terms and Definitions.
- Section 4 – Abbreviations.
- Section 5 – Background information including a description of the provisioning reference architecture, components and interfaces.
- Section 6 – Provisioning overview including logical state transition diagram.
- Section 7 – Provisioning flows for initial power-on, post-power-on, scenarios involving updating services on an MTA endpoint, and limited failure scenarios.
- Section 8 – PacketCable requirements for DHCP [1] option code 60 and option code 177.
- Section 9 – MTA Provisionable attributes (configuration file)
- Section 10 – 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 REFERENCES

2.1 Normative References

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

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

[2] PacketCable MTA MIB, PKT-SP-MIB-MTA-I03-0021018, Cable Television Laboratories, Inc., October 18, 2002. http://www.PacketCable.com./

[3] PacketCable SIGNALING MIB, PKT-SP-MIB-SIG-I04-021018, Cable Television Laboratories, Inc., October 18, 2002. http://www.PacketCable.com./

[4] PacketCable Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I04-021018, Cable Television Laboratories, Inc., October 18, 2002, http://www.PacketCable.com./

[5] PacketCable Security Specification, PKT-SP-SEC-I06-021018, Cable Television Laboratories, Inc., October 18, 2002, http://www.PacketCable.com./

[6] Data-Over-Cable Service Interface Specification, Radio Frequency Interface Specification. SP-RFIv1.1-I09-020830, Cable Television Laboratories, Inc. http://www.cablemodem.com/

2.2 Informative References

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

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

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

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

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

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

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

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

[15] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, CMCI, DOCSIS SP-CMCI-I06-010829, Cable Television Laboratories, Inc., August 29, 2001, http://www.cablemodem.com/

[16] IETF RFC1449, SNMPv2-TM.

[17] IETF RFC1903, SNMPv2-TC.

[18] IEFT RFC 2574, Use-base Security Model (USM) for Version 3 of the SNMPv3.

[19] Data-Over-Cable Service Interface Specifications, Operations Support System Interface Specification Radio Frequency Interface SP-OSSIv1.1-I04-01829, Cable Television Laboratories, Inc., August 29, 2001, http://www.cablemodem.com/

[20] IETF RFC 821, Simple Mail Transfer Protocol.

[21] IETF RFC 1157, A Simple Network Management Protocol (SNMP).

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

[23] IETF RFC 2349, TFTP Timeout Interval and Transfer Size Options.

[24] IETF RFC 1945, IETF RFC-2068, HTTP 1.0 and 1.1.

[25] IETF RFC 2475, An Architecture for Differentiated Services.

[26] PacketCable Audio/Video Codecs Specification, PKT-SP-CODEC-I04-021018, Cable Television Laboratories, Inc., October 18, 2002. http://www.PacketCable.com./

[27] PacketCable Dynamic Quality of Service Specification, PKT-SP-DQOS-I0-021018, Cable Television Laboratories, Inc., October 18, 2002, http://www.PacketCable.com./

3 TERMS AND DEFINITIONS

PacketCable specifications use the following terms:

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.
A-link	A-Links are SS7 links that interconnect STPs and either SSPs or SCPs. 'A' stands for "Access."
Asymmetric Key	An encryption key or a decryption key used in public key cryptography, where encryption and decryption keys are always distinct.
Audio Server	An Audio Server plays informational announcements in PacketCable network. Media announcements are needed for communications that do not complete and to provide enhanced information services to the user. The component parts of Audio Server services are Media Players and Media Player Controllers.
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 that claims to have given the information.
Authorization	The act of giving access to a service or device if one has permission to have the access.
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.
Cleartext	The original (unencrypted) state of a message or data. Also called plaintext.

Confidentiality	A way to ensure that information is not disclosed to anyone other then the intended parties. Information is encrypted to provide confidentiality. Also known as privacy.
Cryptanalysis	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.
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.
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.
Downstream	The direction from the head-end toward the subscriber location.
Encipherment	A method used to translate plaintext into ciphertext.
Encryption	A method used to translate plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or Multipoint Conference Unit.
Errored Second	Any 1-second interval containing at least one bit error.
Event Message	A message capturing a single portion of a connection.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
Flow [DOCSIS Flow]	A unidirectional sequence of packets associated with a Service ID and a QoS. Multiple multimedia streams may be carried in a single DOCSIS Flow. Also known as a DOCSIS-QoS "service flow")
Flow [IP Flow]	A unidirectional sequence of packets identified by OSI 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.
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 to the edge of the PacketCable network.
H.323	An ITU-T standard for transmitting and controlling audio and video information. The H.323 recommendation 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.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local Access and Transport Area.
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.
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.
Keying Material	A set of cryptographic keys and their associated parameters, normally associated with a particular run of a security protocol.
Keyspace	The range of all possible values of the key for a particular cryptographic algorithm.
Latency	The time, expressed in quantity of symbols, taken for a signal element to pass through a device.
Link Encryption	Cryptography applied to data as it travels on data links between the network devices.
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.
Nonce	A random value used only once that 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.
Off-Net Call	A communication connecting a PacketCable subscriber to a user on the PSTN.
One-way Hash	A hash function that has an insignificant number of collisions upon output.
On-Net Call	A communication placed by one customer to another customer entirely on the PacketCable Network.
Plaintext	The original (unencrypted) state of a message or data. Also called cleartext.
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, thereby eliminating the need for a host to support the service.
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 an 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 user's private key is kept secret and is the only key that can decrypt messages sent encrypted by the user's public key.
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 generated with the corresponding root private key.
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.
Signed and Sealed	An "envelope" of information which has been signed with a digital signature and sealed using encryption.
Subflow	A unidirectional flow of IP packets characterized by a single source and destination IP address and single 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.
Transit Delays	The time difference between the instant at which the first bit of a Protocol Data Unit (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 that carries user media content and may carry voice signaling (M_F, R_2, etc.).
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.
Upstream	The direction from the subscriber location toward the headend.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.

4 ABBREVIATIONS

PacketCable specifications use the following abbreviations.

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard. A block cipher, used to encrypt the media traffic in PacketCable.
AF	Assured Forwarding. This is a DiffServ Per Hop Behavior.
AH	Authentication header. An IPSec security protocol that provides message integrity for complete IP packets, including the IP header.
AMA	Automated Message Accounting. A standard form of call detail records (CDRs) developed and administered by Bellcore (now Telcordia Technologies).
ASD	Application-Specific Data. A field in some Kerberos key management messages that carries information specific to the security protocol for which the keys are being negotiated.
AT	Access Tandem
ATM	Asynchronous Transfer Mode. A protocol for the transmission of a variety of digital signals using uniform 53-byte cells.
BAF	Bellcore AMA Format, also known as AMA.
BCID	Billing Correlation ID

BPI+	Baseline Privacy Plus Interface Specification. The security portion of the DOCSIS 1.1 standard that runs on the MAC layer.
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. The part of the CMS that maintains the communication state, and controls the line side of the communication.
CBC	Cipher Block Chaining Bode. 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
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
CIR	Committed Information Rate
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. This is one example of an Application Server.
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.
CMSS	CMS-to-CMS Signaling
Codec	COder-DECoder
COPS	Common Open Policy Service protocol. 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 configuration file.
CSR	Customer Service Representative
DA	Directory Assistance
DE	Default. This is a DiffServ Per Hop Behavior.
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DHCP-D	DHCP Default. Network Provider DHCP Server
DNS	Domain Name Service
DOCSIS™	Data-Over-Cable Service Interface Specifications
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. Assigned on the fly for each communication depending on the QoS requested.
DSCP	DiffServ Code Point. A field in every IP packet that 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.
DSFID	Downstream Service Flow ID. See SFID
DTMF	Dual-tone Multi Frequency (tones)
EF	Expedited Forwarding. A DiffServ Per Hop Behavior.
E-MTA	Embedded MTA. A single node that contains both an MTA and a cable modem.
EO	End Office

ESP	IPSec Encapsulating Security Payload. Protocol that provides both IP packet encryption and optional message integrity, not covering the IP packet header.
ETSI	European Telecommunications Standards Institute
FEID	Financial Entity ID
FGD	Feature Group D signaling
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 821 for details.
GC	Gate Controller
GTT	Global Title Translation
HFC	Hybrid Fiber/Coax coaxial able). An 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.
HMAC	Hashed Message Authentication Code. A message authentication algorithm, based on either SHA-1 or MD5 hash and defined in IETF RFC 2104.
HTTP	Hypertext 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 on the Internet. See www.ietf.org for details
IKE	Internet Key Exchange. 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 with X.509 certificates for authentication.
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
ISTP	Internet Signaling Transport Protocol
ISUP	ISDN User Part. A protocol within the SS7 suite of protocols that is used for call signaling within an SS7 network.
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union–Telecommunications Standardization Sector
IVR	Interactive Voice Response system
KDC	Key Distribution Center
LATA	Local Access and Transport Area
LD	Long Distance
LIDB	Line Information Database. Contains customer information required for real-time access such as calling card personal identification numbers (PINs) for real-time validation.
LLC	Logical Link Control. 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.
lsb	Least significant bit
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
MCU	Multipoint Conferencing Unit
MD5	Message Digest 5. A one-way hash algorithm that maps variable length plaintext into fixed-length (16 byte) ciphertext.

MDCP	Media Device Control Protocol. 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	Media Gateway. Provides the bearer circuit interfaces to the PSTN and transcodes the media stream.
MGC	Media Gateway Controller. The overall controller function of the PSTN gateway. Receives, controls and mediates call-signaling information between the PacketCable and PSTN.
MGCP	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF 2705.
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 Message Authentication Code (MAC).
MMC	Multi-Point Mixing Controller. A conferencing device for mixing media streams of multiple connections.
MSB	Most Significant Bit
MSO	Multi-System Operator. A cable company that operates many head-end locations in several cities.
MSU	Message Signal Unit
MTA	Multimedia 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. A set of two protocols (MTP 2 and 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. This layer provides services to establish a path between open systems.
NCS	Network Call Signaling
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 numbers (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. Defines the analog color television broadcast standard used today in North America.
OID	Object Identifier
OSP	Operator Service Provider
OSS	Operations Systems Support. The back-office software used for configuration, performance, fault, accounting, and security management.
OSS-D	OSS Default. Network Provider Provisioning Server.
PAL	Phase Alternate Line. The European color television format that evolved from the American NTSC standard.
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.
PDU	Protocol Data Unit
PHB	Per-Hop Behavior

PHS	Payload Header Suppression. A DOCSIS technique for compressing the Ethernet, IP, and UDP headers of RTP packets.
PKCROSS	Public-Key Cryptography for Cross-Realm Authentication. Utilizes PKINIT for establishing the inter-realm keys and associated inter-realm policies to be applied in issuing cross-realm service tickets between realms and domains in support of Intradomain and Interdomain CMS-to-CMS signaling (CMSS).
PKCS	Public-Key Cryptography Standards. Published by RSA Data Security Inc. These Standards describe 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	Public-Key Cryptography for Initial Authentication. The extension to the Kerberos protocol that provides a method for using public-key cryptography during initial authentication.
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
QCIF	Quarter Common Intermediate Format
QoS	Quality of Service. Guarantees network bandwidth and availability for applications.
RADIUS	Remote Authentication Dial-In User Service. An internet protocol (IETF 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	Rivest Cipher 4. A variable length stream cipher. Optionally 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	Registered Jack-11. A standard 4-pin modular connector commonly used in the United States for connecting a phone unit into a wall jack.
RKS	Record Keeping Server. The device which collects and correlates the various Event Messages.
RSA	A public-key, or asymmetric, cryptographic algorithm used to provide authentication and encryption services. RSA stands for the three inventors of the algorithm; Rivest, Shamir, Adleman.
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 Transport Protocol. A protocol for encapsulating encoded voice and video streams. Refer to IETF RFC 1889.
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 DOCSIS Baseline Privacy Plus Interface (BPI+) security protocol.
SCCP	Signaling Connection Control Part. A protocol within the SS7 suite of protocols that provides two functions in addition to those provided within MTP. The first function is the ability to address applications within a signaling point. The second function is Global Title Translation.

SCP	Service Control Point. A Signaling Point within the SS7 network, identifiable by a Destination Point Code that provides database services to the network.
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SDU	Service Data Unit. Information delivered as a unit between peer service access points.
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 variant 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.
SIP	Session Initiation Protocol. An application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants.
SIP+	Session Initiation Protocol Plus. An extension to SIP.
S-MTA	Standalone MTA. A single node that contains an MTA and a non-DOCSIS MAC (e.g., ethernet).
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SS7	Signaling System number 7. An architecture and set of protocols for performing out-of-band call signaling with a telephone network.
SSP	Service 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. A node within an SS7 network that routes signaling messages based on their destination address. This is essentially a packet switch for SS7. It may also perform additional routing services such as Global Title Translation.
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. A sub-system of the KDC used to grant Kerberos tickets.
TGW	Telephony Gateway
TIPHON	Telecommunications and Internet Protocol Harmonization Over Network
TLV	Type-Length-Value. A 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.
TSG	Trunk Subgroup

USFID	Upstream Service Flow ID. See SFID
UDP	User Datagram Protocol. A connectionless protocol built upon Internet Protocol (IP).
VAD	Voice Activity Detection
VBR	Variable Bit Rate
VoIP	Voice over IP

5 BACKGROUND

5.1 Service Goals

Cable operators are interested in deploying high-speed data communications systems on cable television systems. Cable operators and Cable Television Laboratories, Inc. (on behalf of the CableLabs® member companies), have prepared 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 [6]. This is shown in simplified form in Figure 1.

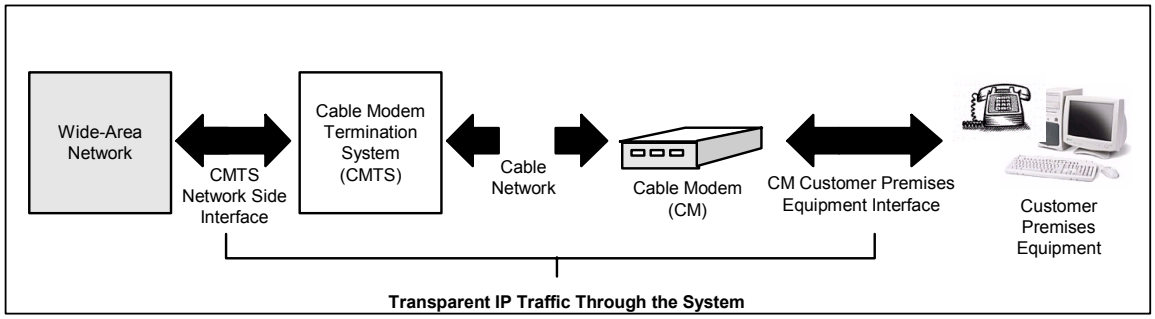


Figure 1. Transparent IP Traffic Through the Data-Over-Cable System

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). 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.

5.2 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 two IP addresses; an IP address for the CM component, and a different IP address for the MTA component. The embedded-MTA MUST have two MAC addresses, one MAC address for the CM component, and a different MAC address for the MTA-component.
- PacketCable requires a unique FQDN for the MTA-component in the embedded-MTA. This FQDN MUST 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. 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 use DHCP Option-12 and Option-15 to deliver the MTA FQDN to the E-MTA.
- 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.
- The embedded-MTA is outside the PacketCable network trust boundary as defined in the PacketCable architecture document [14].
- PacketCable 1.0 MUST support DOCSIS 1.1 software download as defined in [6]. The DOCSIS 1.1 software download process supports the downloading of a single file to the cable modem or embedded MTA. A single DOCSIS 1.1 software download MUST be used to upgrade code for both DOCSIS and PacketCable software functions.
- 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).

5.3 PacketCable Reference Architecture

Figure 2 shows the reference architecture for the PacketCable 1.0 Network. Refer to the PacketCable Architecture Document [14] for more detailed information on this reference architecture.

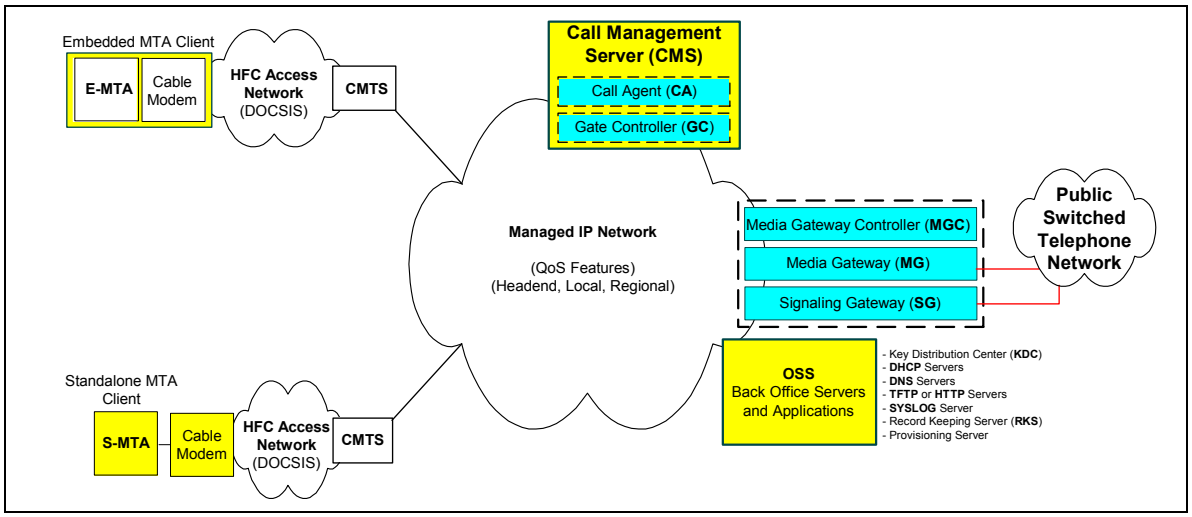


Figure 2. PacketCable 1.0 Network Component Reference Model

5.4 Components and Interfaces

This interface identifies specific requirements in the DHCP server and the client for IP assignment during the MTA initialization process. This figure represents the components and interfaces discussed in this document. All the PacketCable specifications have a similar diagram indicating which interfaces of the PacketCable Architecture are affected by a particular specification.

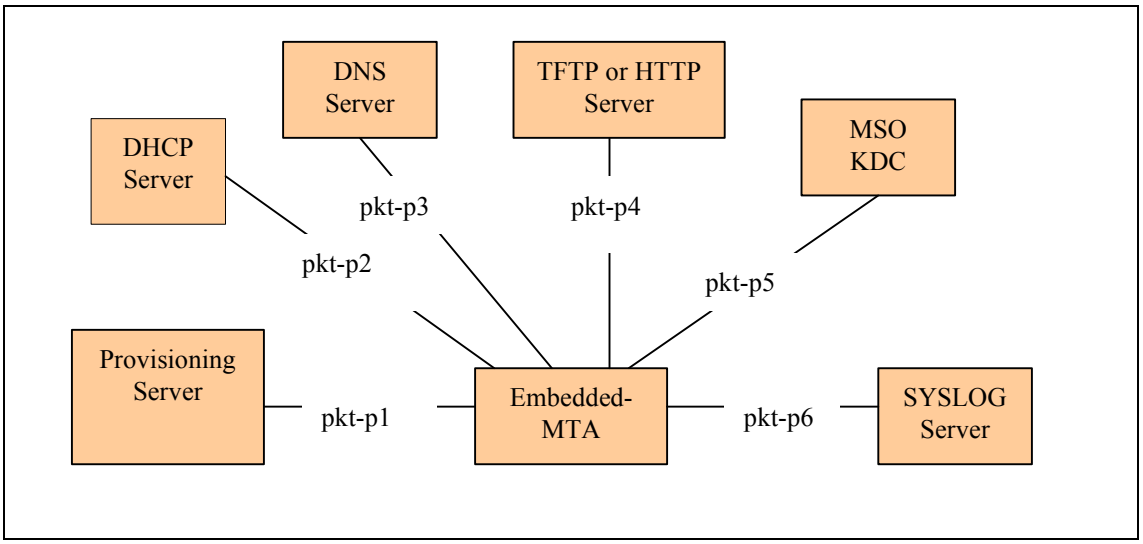


Figure 3. PacketCable Provisioning Interfaces

5.4.1 MTA

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

5.4.1.1 MTA Security Requirements

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

- 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-endpoint basis, unless all endpoints are configured to same CMS.
- CMS Kerberos Principal Name is not explicitly configured in the MTA endpoints. The MTA MUST be able to determine the CMS Kerberos Principal Name based on the CMS FQDN, as specified in [5].
- For each unique pair of CMS Kerberos principal Name / Kerberos Realm assigned to an endpoint, the MTA MUST obtain a single Kerberos ticket [5]. If the MTA already has a valid Kerberos ticket for that CMS, the MTA MUST NOT request an additional Kerberos ticket for that CMS. (Unless the expiration time of the current Kerberos ticket <= current time + PKINIT Grace Period, in which case the MTA MUST obtain a fresh ticket for the same CMS.)
- In the case that a CMS FQDN maps to multiple IP addresses, the MTA MUST initially establish a pair of IPSEC Security Associations with one of the IP addresses returned by the DNS server. The MTA MAY also initially establish IPSEC Security Associations with the additional CMS IP addresses. Please refer to [5] for more information.
- During the MTA initialization, if the MTA already has a pair of active Security Associations (inbound and outbound) with a particular CMS IP address, the MTA MUST NOT attempt to establish additional Security Associations with the same IP address.

5.4.1.2 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.

5.4.2 Provisioning Server

The Provisioning Server is made up of the following components:

- Provisioning Application - The Provisioning Application is responsible for coordinating the embedded-MTA provisioning process. This application has an associated SNMP Entity.
- Provisioning SNMP Entity – The provisioning SNMP entity MUST include a trap/inform handler for provisioning enrollment and the provisioning status traps/informs as well as a SNMP engine for retrieving device capabilities and setting the TFTP filename and access method. Refer to the PacketCable MTA MIB [2] 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.

5.4.3 MTA to Telephony Syslog Server

E-MTA MUST receive its Telephony Syslog Server IP address in the DHCP OFFER, option 7 (RFC-2132). The length of the option MUST be 4 octets. The value of the option MUST be one of the following:

- 0.0.0.0 – means that Syslog logging for MTA is turned off

- FF.FF.FF.FF – means that address of the Syslog Server for DOCSIS MUST be used.
- Any other value – represents the IP address of the Telephony Syslog Server.

The MTA's SYSLOG message (when used) MUST be sent in the following format:

<level>MTA[vendor]:<eventId>text

Where:

level – ASCII presentation of the event priority, enclosed in angle brackets, which is constructed as a logical or of the default Facility (128) and event priority (0-7). The resulted level has the range between 128 and 135.

vendor – Vendor name for the vendor-specific SYSLOG messages or PACKETCABLE for the standard PACKETCABLE messages.

eventId – ASCII presentation of the INTEGER number in HEX format, enclosed in angle brackets, which uniquely identifies the type of event.

Example: Syslog event for AC power failure in the MTA

<132>MTA[CableLabs]:<65535>AC Power Fail·

In case of failure, the result of each Provisioning Flow SHOULD be reported as a Provisioning Event (list of events is present in the Appendix A).

5.4.4 MTA to DHCP Server

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

- Both the DHCP server and the embedded-MTA MUST support DHCP option code 7, 12, 15, 60 and DHCP option code 177 as defined in this document. Option code 12 and 15 MUST be FQDN which MUST be resolved by DNS server.
- The DHCP server MUST accept and support broadcast and unicast messages per RFC 2131 from the MTA DHCP client.
- The DHCP server MUST 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.

5.4.5 MTA to Provisioning Application

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

- The MTA MUST generate a correlation ID — an arbitrary value that will be exchanged as part of the device capability data to the Provisioning Application. This value is used as an identifier to correlate related events in the MTA provisioning sequence.
- The Provisioning Application MUST provide the MTA with its MTA configuration data file. The MTA configuration file is specific to the MTA-component of the embedded-MTA and separate from the CM-component's configuration data file.
- The configuration data file format is TLV binary data suitable for transport over the specified TFTP or HTTP access method.
- The Provisioning Application MUST have the capability to configure the MTA with different data and voice service providers.
- The Provisioning Application MUST provide secure SNMP access to the device.

- The Provisioning Application MUST support online incremental device/subscriber provisioning using SNMP with security enabled.
- MTA MUST Specify all of its Capabilities in DHCP Option-60 in accordance with section 8.2.
- Provisioning Application MUST NOT assume any Capabilities, which do not have default values. In case if Capabilities supplied by the MTA are not consistent in format and/or in number and/or in values, the Provisioning Application MUST use the other means to identify the MTA's capabilities (e.g. SNMPv3 if possible).

5.4.6 MTA to CMS

Signaling is the main interface between the MTA and the CMS. Refer to the PacketCable signaling document [4] 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.

5.4.7 MTA to Security Server (KDC)

The interface between the MTA and the Key Distribution Center (KDC) MUST conform to the PacketCable security specification [5].

AP-REQ/REP exchange back off and retry mechanism of the Kerberized SNMPv3 key negotiation defined in [5] is controlled by the values deliver by "suboption-11" of the DHCP Option 177 (see section 8.1.7).

AS-REQ/REP exchange backoff and retry mechanism of the Kerberized SNMPv3 key negotiation defined in [5]is controlled by the values deliver by "suboption-10" of the DHCP Option 177 (see section 8.1.6) or by the default values of the corresponding MIB objects in the Realm Table if "suboption-10" is not present in the DHCP Option 177.

5.4.8 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.

5.4.9 DOCSIS extensions for MTA Provisioning

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

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

6 PROVISIONING OVERVIEW

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

6.1 Device Provisioning

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

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 optional. Therefore the configuration file is "signed" and may be "sealed". Please refer to [5] for further information.

Please refer to section 5.4.1 for provisioning rules related to security associations.

6.2 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. This allows subsequent call signaling to be protected under the established security association.

Endpoint provisioning will employ the Kerberos CMS Ticket the MTA obtained during subscriber enrollment. Please refer to [5] for further information.

6.3 MTA 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. The following MTA state transitions do not specify the number of retry attempts or retry time out values.

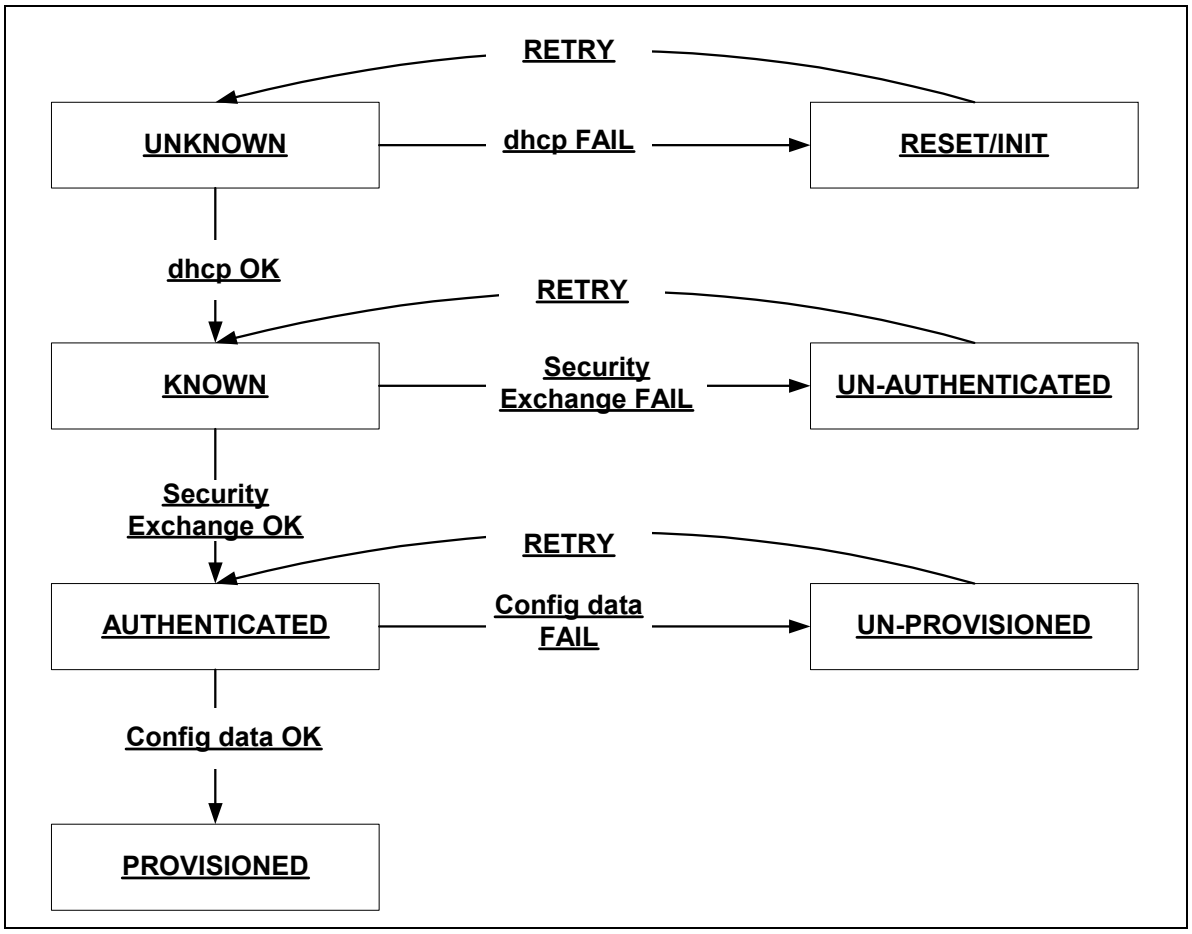


Figure 4. Device States and State Transitions

7 PROVISIONING FLOWS

7.1 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], HTTP, and SNMP 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 [5] for the security message flows.

7.2 Embedded-MTA Power-On Initialization Flows

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

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

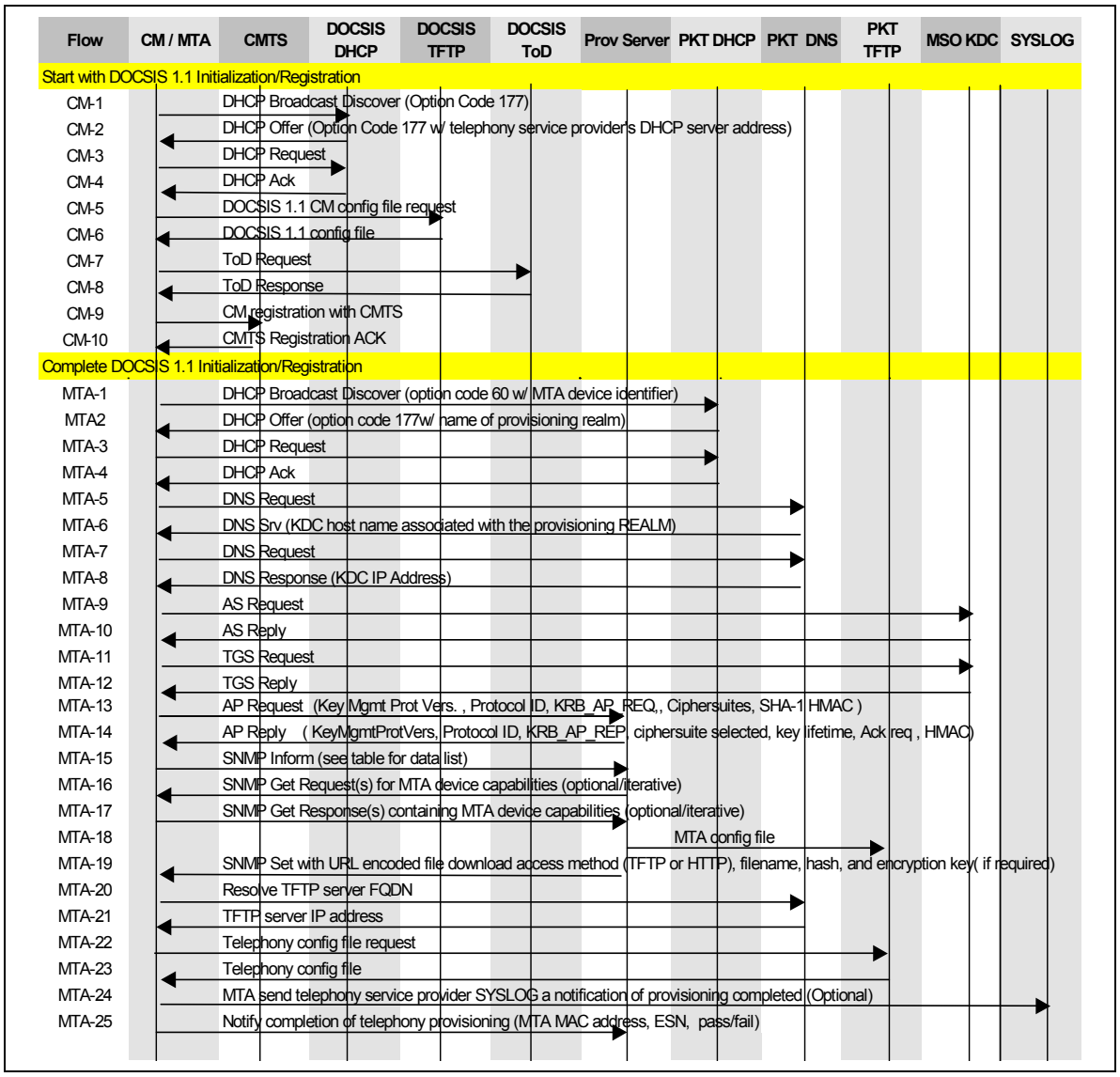


Figure 5. Embedded-MTA Power-on Initialization Flow

Flow	Embedded-MTA Power-On Initialization Flow Description	Normal Flow Sequencing	Proceed to here if this step fails
NOTE: Refer to the DOCSIS 1.1 specification for a complete description of flows CM1- CM10.			
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. This message includes Option code 60 (Vendor Specific Option) in the format "docsis1.1:xxxxxxx". This message MUST request Option 177 in Option 55, the request parameter list. REQ2652 The remainder of this message MUST conform to the DHCP discover data as defined in the DOCSIS 1.1 specification.	Initial MUST Step in Sequence	Per DOCSIS
CM2	The DOCSIS DHCP Server, if it has been configured to support MTA devices, MUST include Option 177 code with sub-option 1 and, possibly, sub-option 2 as per section 8.1. If it is configured to prevent the MTA portion of the device from provisioning, then sub-option 1 in Option 177 code MUST be set to 0.0.0.0. DOCSIS DHCP Servers without any prior knowledge of MTA devices MAY respond with DHCP OFFERS without including option 177.	CM2 MUST occur after CM1 Completion	Per DOCSIS
CM3	Upon receiving a DHCP OFFER, the CM MUST check for the requested option 177. If it is not present then it MUST retry the DHCP DISCOVER process (CM1) exponentially for 3 attempts [e.g. 2, 4, 8 second intervals]. Upon failing to receive any DHCP OFFER with option 177 after the exponential retry mechanism it MUST consider OFFERs without option code 177 and accept one of them as per the DHCP specification [1]. The client device (CM) MUST then send a DHCP REQUEST broadcast message to the DHCP server whose OFFER it accepted as specified in the DHCP specification [1].	CM3 MUST occur after CM2 Completion	Per DOCSIS
CM4	The DHCP server sends the client device cable modem component a DHCP ACK message to confirm acceptance of the offered data. Upon receiving the DHCP ACK, the CM MUST check again for option 177. The absence of option 177 in the DHCP ACK message, that was accepted by the CM, implies that it MUST not initialize the embedded MTA. The presence of option 177 implies that it MUST initialize the MTA and pass suboption 1 and, possibly, suboption 2. If the option content of this DHCP ACK differs with the preceding DHCP OFFER, the option content of this DHCP ACK MUST be treated as authoritative (per RFC 2131).	CM4 MUST occur after CM3 Completion	Per DOCSIS

Flow	Embedded-MTA Power-On Initialization Flow Description	Normal Flow Sequencing	Proceed to here if this step fails
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.	CM5 – CM10 MUST occur after CM4 completion	Per DOCSIS
MTA1	DHCP Broadcast Discover The MTA MUST send a broadcast DHCP Discover message. This message MUST include option code 60 (Vendor Specific Option) in the format "pktc1.0:xxxxxx" and MUST request in option 55 the following: 7, 12, 15, 177. If suboption1 in option code 177 (passed by the CM to the MTA) contains 0.0.0.0 then the MTA MUST not attempt to provision and remain dormant until it is reinitialized by the CM.	MTA1 MUST not occur before completion of CM4	If failure per DHCP protocol repeat MTA1
MTA2	DHCP Offer If the MTA at this stage receives multiple valid DHCP OFFERs (during its wait period as per RFC 2131) and is ready to choose a valid OFFER, it MUST check for the contents of suboption 3 If all the valid DHCP OFFERs contain 0.0.0.0 then the MTA MUST not further the DHCP process and shutdown till it is reinitialized. If, however, among the valid, acceptable DHCP OFFERs there are OFFERs with a non-zero value in sub-option 3 the MTA MUST further attempt the DHCP process and choose a valid OFFER with a non-zero sub-option 3 The MTA MUST accept the DHCP offer from the primary or secondary DHCP servers returned in option code 177 in sub-options 1 and 2 from CM2. The DHCP offer MUST include the following options: 7, 12, 15, 177 with sub-options 3, 4, and 6. NOTE: Option 177 MAY also includes sub-options 5, 7, 8, 9, 10 and 11. If an MTA supports TGTs and receives sub-option 7 = FALSE, it MUST NOT request TGTs. If an MTA supports TGTs and receives sub-option 7 = TRUE, it MUST request TGTs. MTAs that do not support TGTs MUST ignore sub option 7	MTA2 MUST occur after MTA1 completion	If failure per DHCP protocol return to MTA1

Flow	Embedded-MTA Power-On Initialization Flow Description	Normal Flow Sequencing	Proceed to here if this step fails
MTA3	DHCP Request The MTA MUST accept the DHCP offer from the primary or secondary DHCP servers returned in option code 177 in sub-options 1 and 2 from CM2. If sub-option 1 contained 255.255.255.255, then the MTA MUST use logic defined in DHCP [1] to select an offer. The MTA MUST reject offers that do not contain mandatory options: 7, 12, 15, 177 with sub-options 3, 4, and 6. In any case, the MTA component MUST send a DHCP REQUEST broadcast message to accept the DHCP offer. Refer to Section 2 [1] for more details concerning the DHCP protocol	MTA3 MUST occur after MTA2 completion	If failure per DHCP protocol return to MTA1
MTA4	DHCP Ack The DHCP server sends the client device's MTA component a DHCP ACK message which MUST contain the IPv4 of the MTA and MUST contain the FQDN of the MTA. If the option content of this DHCP ACK differs with the preceding DHCP OFFER, the option content of this DHCP ACK MUST be treated as authoritative (per RFC 2131).	MTA4 MUST occur after MTA3 completion	If failure per DHCP protocol return to MTA1
MTA5	DNS Srv Request The MTA requests the MSO KDC host name for the Kerberos realm.	MTA5 MUST occur after MTA4 completion	MTA1
MTA6	DNS Srv Reply Returns the MSO KDC host name associated with the provisioning REALM.	MTA6 MUST occur after MTA5 completion	MTA1
MTA7	DNS Request The MTA now requests the IP Address of the MSO KDC.	MTA7 MUST occur after MTA6 completion	MTA1
MTA8	DNS Reply The DNS Server returns the IP Address of the MSO KDC.	MTA8 MUST occur after MTA7 completion	MTA1
MTA9	AS Request The AS Request message is sent to the MSO KDC to request a Kerberos ticket.	If MTA9 occurs, it MUST occur after MTA8 completion.	MTA1
MTA10	AS Reply The AS Reply Message is received from the MSO KDC containing the Kerberos ticket. NOTE: The KDC must map the MTA MAC address to the FQDN before send the AS Reply.	MTA10 MUST occur after MTA9 completion	MTA1
NOTE: Flows MTA11– MTA12 are optional is some cases, please reference the Security Specification [5]. NOTE: Option 177 may also include 5, 7, and 8.			

Flow	Embedded-MTA Power-On Initialization Flow Description	Normal Flow Sequencing	Proceed to here if this step fails
MTA11	TGS Request If MTA obtained TGT in MTA10, the TGS Request message is sent to the MSO KDC.	MTA11 MUST occur after MTA10 completion	MTA1
MTA12	TGS Reply The TGS Reply message is received from the MSO KDC.	MTA12 MUST occur after MTA11 completion	MTA1
MTA13	AP Request The AP Request message is sent to the Provisioning Server to request the keying information for SNMPv3.	MTA13 MUST occur after MTA12 or MTA 10 completion	MTA1
MTA14	AP Reply The AP Reply message is received from the Provisioning Server containing the keying information for SNMPv3. NOTE: The SNMPv3 keys must be established before the next step using the information in the AP Reply.	MTA14 MUST occur after MTA13 completion	MTA1
MTA15	SNMP Inform The client device MTA component sends the PROV_SNMP_ENTITY a SNMPv3 INFORM requesting enrollment. The receipt of the inform is acknowledged by the response message as defined in RFC 2574 [18]. The FQDN of this PROV_SNMP_ENTITY is contained in the PacketCable DHCP offer message. The following information MUST be in the "PktcMtaProvisioningEnrollment object: Software Version Device Identifier String (pktc1.0:xxxxxx) MAC address Telephony Provisioning Correlation ID Please refer to the "PktcMtaProvisioningEnrollment" object in the MTA MIB [2] for a detailed description of these data values. The PROV_SNMP_ENTITY notifies the PROV_APP that the MTA has entered the management domain.	MTA15 MUST occur after MTA14 completion	If failure per SNMP protocol return to MTA1. SNMP server MUST send response to SNMP-INFORM.
NOTE: The provisioning server can reset the MTA at this point in the flows. The MTA is part of the security domain and MUST respond to management requests, the SNMP INFORM of MTA15 is the indicator, see section 5.4.1.2.			

Flow	Embedded-MTA Power-On Initialization Flow Description	Normal Flow Sequencing	Proceed to here if this step fails
MTA16	SNMP Get Request (Optional) If any additional MTA device capabilities are needed by the PROV_APP, the PROV_APP requests these from the MTA via SNMPv3 Get Requests. This is done by having the PROV_APP send the PROV_SNMP_ENTITY a "get request" Iterative: The PROV_SNMP_ENTITY sends the MTA one or more SNMPv3 GET requests to obtain any needed MTA capability information. The Provisioning Application may use a GETBulk request to obtain several pieces of information in a single message.	MTA16 is optional, can occur after MTA15 completion	N/A
MTA17	SNMP Get Response 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.	MTA17 MUST occur after MTA16 completion if MTA16 is performed	N/A
MTA18	This Protocol is not defined by PacketCable The PROV_APP MAY use the information from MTA16 and MTA17 to determine the contents of the MTA Configuration Data file. Mechanisms for sending, storing and, possibly, creating the configuration file are outlined in MTA19.	MTA18 SHOULD occur after MTA15 completion unless MTA16 is performed, then it SHOULD be after MTA17 has completed	N/A

Flow	Embedded-MTA Power-On Initialization Flow Description	Normal Flow Sequencing	Proceed to here if this step fails
MTA19	SNMP Set The PROV_APP MAY create the configuration file at this point, or send a predefined one. A hash MUST be run on the contents of the configuration file. The configuration file MAY be encrypted The hash and the encryption key (if the configuration file is encrypted) MUST be sent to the MTA. The PROV_APP MUST store the configuration file on the appropriate TFTP server. The PROV_APP then instructs the PROV_SNMP_ENTITY to send an SNMP Set message to the MTA containing the URL-encoded file access method and filename, the hash of the configuration file, and the encryption key (if the configuration file is encrypted). NOTES: In the case of file download using the HTTP access method, the filename MUST be URL-encoded in the following format: http://[IPv4] or FQDN of access server/ mta-config-filename In the case of file download using the TFTP access method, the filename MUST be URL-encoded in the following format: tftp://[IPv4] or FQDN of access server/mta-config-filename	MTA19 MUST occur after MTA18 completion	If failure per SNMP protocol return to MTA1
MTA20	DNS Request If the URL-encoded access method contains a FQDN instead of an IPv4 address, the MTA MUST use the service provider network's DNS server to resolve the FQDN into an IPv4 address of either the TFTP Server or the HTTP Server.	MTA20 MUST occur after MTA19 completion if FQDN is used	If failure per DNS protocol return to MTA1
MTA21	DNS Reply DNS Response: DNS server returns the IP address against MTA20 DNS request.	MTA21 MUST occur after MTA20 completion if FQDN is used	If failure per DNS protocol return to MTA1
MTA22	TFTP/HTTP Get Request The MTA MUST send the TFTP Server a TFTP Get Request to request the specified configuration data file. In the case of file download using the HTTP access method, the MTA MUST send the HTTP server a request for the specified configuration data file.	MTA22 MUST occur after MTA19 unless FQDN is specified then MUST be after MTA20 – MTA21	If failure per TFTP or HTTP protocols, return to MTA1

Flow	Embedded-MTA Power-On Initialization Flow Description	Normal Flow Sequencing	Proceed to here if this step fails
MTA23	TFTP/HTTP Get Response The TFTP Server MUST send the MTA a TFTP Response containing the requested file. In the case of file download using the HTTP access method, the HTTP server MUST sends the MTA a response containing the requested file. The hash of the configuration file is calculated and compared to the value received in step MTA19. If encrypted, the configuration file MUST be decrypted. If the MTA does not complete this step in the time specified by the MIB object 'pktcMtaDevProvisioningTimer' the device MUST return to MTA1. Refer to section 9.1 for MTA configuration file contents.	MTA23 MUST occur after MTA22 completion.	If the configuration file download failed per TFTP or HTTP protocols, return to MTA1. Otherwise, proceed to MTA24 or MTA25, and send the failed response if the MTA configuration file itself is in error.
MTA24	SYSLOG Notification The MTA SHOULD send 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 section 5.4.3.	MTA24 is optional, can occur after MTA23 completion if SYSLOG used	A vendor MAY consider returning to MTA15, repeating until it is determined to be a hard failure and then MUST continue to MTA25.
MTA25	SNMP Inform The MTA MUST send the PROV_SNMP_ENTITY an SNMP INFORM containing a "provisioning complete" notification. The receipt of the inform is acknowledged by the response message as defined in RFC 2574 [18]. The following information MUST be in the "PktcMtaProvisioningStatus" object: MAC address Telephony Provisioning Correlation ID Provisioning State 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).	MTA25 MUST occur after MTA24 if SYSLOG is used, otherwise MUST occur after MTA23 completion	MTA MAY generate a Provisioning Failure event notification to the Service Provider's Fault Management server. Provisioning process stops; Manual interaction required. SNMP server MUST send response to SNMP-INFORM.

7.3 Endpoint Provisioning Completion Notifications

Once the pktcMtaProvisioningStatus has been successfully sent to the provisioning server, MTA will set up the necessary security association for the configured realms (KDCs). The MTA NCS signaling software will initiate the establishment of the IPSec security association to the configured CMS clusters. Event notifications are triggered if security associations cannot be established (based on [5]). After the associated security associations are established, the MTA NCS signaling software determines whether a signaling path can be setup with an RSIP message and the associated ACK. Coming from a link down situation, the MTA will send an SNMP Link Up Trap when the RSIP has been properly acknowledged. This indicates that the endpoint is provisioned. If the same CMS is used for multiple endpoints, a SNMP link up message will be sent for each associated endpoint. If not all endpoints use the same CMS, the same process needs to be repeated for each endpoint needing a different configured CMS.

7.4 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).

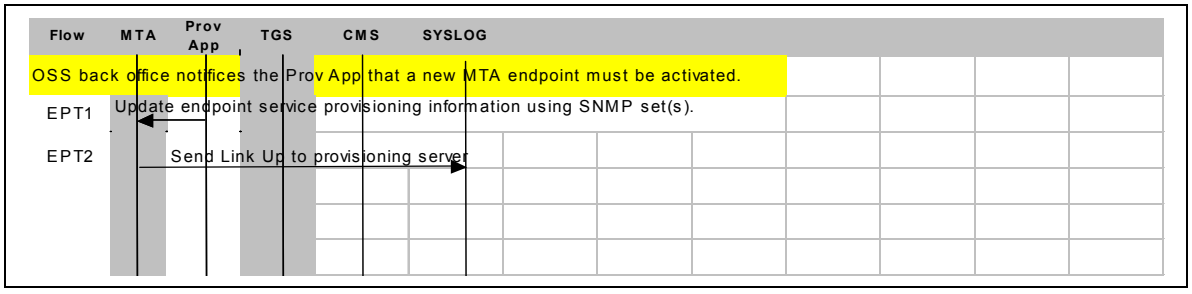
7.4.1 Synchronization of Provisioning Attributes with Configuration File

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 SNMPv3 via the MTA MIB [2]. 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.

7.4.2 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).

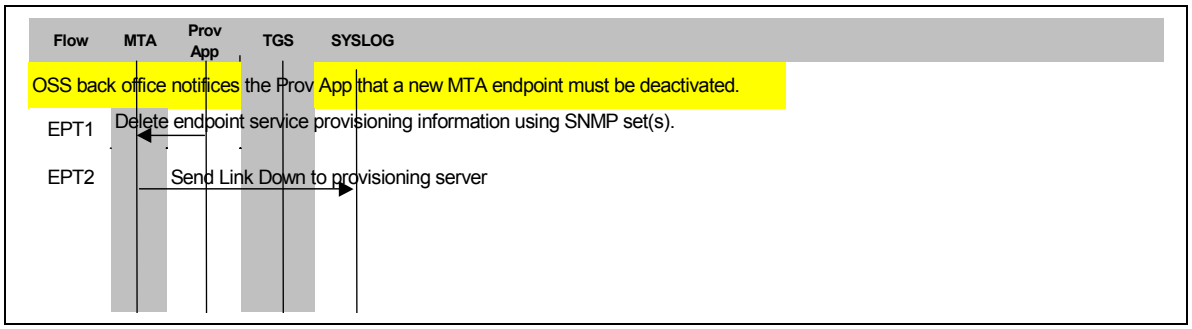
MTA Endpoint services are enabled using SNMPv3 via the MTA MIB [2]. In this example, a subscriber is requesting that additional service be added. This example assumes the service provider's account creation process has been completed, and shows only the applications critical for the flows. For instance, 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	Normal Flow Sequencing
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) and the device port to enable. See section 5.4.1 for details of provisioning rules.	MUST occur after successful power-on initialization flow
EPT2	When an additional endpoint is configured it follows the same procedure as described in section 7.3 with the exception that the process is only executed for the single endpoint configured. If the corresponding security association for new endpoint is already configured and the MTA NSC Signaling Software is currently not in a disconnected state (defined in [4]), the SNMP Link Up Trap will occur immediately after the endpoint is configured. Otherwise, it occurs after the process described in section 7.3 has completed. NOTE: The SNMP Link Up trap is not optional but may be masked using ifLinkUpDownTrapEnable.	EPT2 is Optional if Event Notification is used

7.4.3 Disabling Services on an MTA Endpoint

MTA Endpoint services are disabled using SNMP 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	Normal Flow Sequencing
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.	MUST occur after successful power-on initialization flow
EPT2	A link down trap will occur immediately after the endpoint is unconfigured (i.e., the configuration data for the endpoint is deleted) unless the MTA is currently is a disconnected state with the associated CMS. When an endpoint is unconfigured, the MTA is not required to release any security associations unless explicitly told to do so.	EPT2 is optional if Event Notification is used

7.4.4 Modifying Services on an MTA Endpoint

MTA Endpoint services are modified using SNMPv3Sets to the MTA MIB [2]. 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 request a new Kerberos ticket from the KDC.

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

If the modification to the endpoint changes pktcNcsEndPntConfigCallAgentId and/or pktcNcsEndPntConfigCallAgentUdpPort, the endpoint is taken out of service (SNMP Link Down Trap is sent) followed by the placing the port in service (SNMP Link Up Trap is sent upon completion) with the new parameters. The SNMP Link Up Trap occurs after the sequence in section 7.3 has completed. For all other modifications, no indication is given to the Provisioning Server.

7.5 Behavior During A Disconnected State

Whenever the MTA-CMS association goes from a connected state to a disconnected state (CMS is not responding to MTA CMS Signaling messages), the MTA will send the provisioning server an SNMP Link Down Trap on all the affected endpoints. If a security association between the CMS and the MTA expires while the MTA is in a connected state, the MTA/CMS link will be placed in a disconnected state and the MTA will send an SNMP Link Down Trap for all affected endpoints. Whenever the MTA recovers the security association and the RSIP/Acknowledge sequence occurs, the MTA will send an SNMP Link Up for all affected endpoints.

Whenever the MTA-CMS association recovers from a disconnected state, the MTA will send a SNMP Link Up Trap on all of the affected endpoints.

7.6 Provisioning of the Signaling Communication Path Between the MTA and CMS

The Service Flow(s) for NCS (NCS SF) is(are) not required on the MTA; however, if the NCS SF(s) is(are) implemented and provisioned then the NCS SF(s) MUST be used to provide a signaling communication path between an E-MTA and CMS. One SF MUST be set for all of the MTA's endpoints in each direction.

If NOT provisioned, the signaling communication path will use the primary SF to pass NCS packets.

The following types of DOCSIS Scheduling Services should be used for NCS SF: "Non-Real time Polling Service" (nRTP) or "Best Effort Service" (BE). The other types of services should not be used because the NCS flow characteristics don't match the scheduling characteristics. With either BE or nRTP, the CMTS will give scheduling preference to the NCS flow over the primary flow. With nRTP, the CMTS should also give unicast request opportunities whenever it can so as to allow those flows to avoid contention request collisions.

The creation of the NCS SF MUST occur before Voice Communication Service is activated unless the creation of the SF fails, then Voice Communication Service may be activated and NCS messages will flow over the primary SF.

If the value "pktcSigServiceClassNameMask" MIB Object is not zero and "pktcSigServiceClassNameUS" and "pktcSigServiceClassNameDS " MIB Objects are not empty, then NCS SF MUST be created.

If the value of "pktcSigServiceClassNameUS" or "pktcSigServiceClassNameDS" is set to empty string, then corresponding NCS SF MUST be deleted if it currently exists. After the NCS SF is deleted, and if Voice Communication Service is Enabled, then primary SF for NCS packets will be used instead. If the SNMP Manager sets the object to a value which is not empty string, the NCS SF MUST be created using the corresponding Service Class name.

If Voice Communication Services become Disabled for all end-points of the MTA, then the NCS SF SHOULD be deleted.

If an MTA becomes disabled (pktcMtaDevEnabled is set to FALSE), then the NCS SF SHOULD be deleted (if it exists).

The "pktcSigNcsServiceFlowState" MIB Object MUST indicate the state of the NCS SF according to the Object's description. The E-MTA MUST create the Call Signaling Service Flow using the following steps:

- The E-MTA MUST issue a DSA_Request message to the CMTS for the upstream direction. The DSA-REQ message MUST include the SCN defined in the "pktcSigServiceClassNameUS" MIB Object. If the Service Class Name for the upstream direction is an empty string than the MTA MUST NOT request creation of a service flow.
- The E-MTA MUST issue a DSA_Request message to the CMTS for the Downstream Direction. The DSA-REQ message MUST include the SCN defined in the "pktcSigServiceClassNameDS" MIB Object. [1]
- If any of the above steps result in an error then "pktcSigNcsServiceFlowState" MIB Object MUST be set to the "error" state. An Event Log SHOULD be sent to the SYSLOG Server.

Each DSA message MUST include the resolved IP address for the CMS(s) in the 'IP Destination Address' and 'IP Source Address' for the upstream and downstream service flow creation respectively. A Call Signaling Service flow MAY contain more than one classifier.

[1] DSA-Request for upstream and downstream may be combined as in [18].

7.7 MTA Replacement

PacketCable 1.0 has no requirement to specify MTA replacement procedures. However, the provisioning sequence flows detailed within this document provide sufficient coverage and flexibility to support replacement. In fact, the initialization sequence for a replacement MTA could be the same as the original MTA's first time initialization. Back office procedures related to migration of subscriber profiles from one MTA to another are specific to individual service provider's network operations. As a result of this wide variance, discussion of these back office procedures are beyond the scope of PacketCable 1.0.

7.8 Temporary Signal Loss

If the CM or DOCSIS reset for any reason the MTA will also reset and reinitialize (this will impact calls in progress).

8 DHCP OPTIONS

DHCP is used to obtain IPv4 addresses for both the CM and the MTA. The CM and MTA requirements for DHCP Option Codes 177 and 60 are detailed in section 8.1 and 8.2. These DHCP options are currently defined in a draft proposal submitted to the Internet Engineering Task Force (IETF) DHCP committee [13].

8.1 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 7 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-options 1 and 2 identify the PacketCable network DHCP server, sub-option 3 identifies the PacketCable service provider's SNMP entity, sub-options 4 and 5 identify the primary and secondary PacketCable network DNS servers, sub-option 6 identifies the Kerberos Realm Name of the SNMP entity which belongs in the provisioning realm, and sub-option 7 indicates the MTA should get its TGT when true. Sub-option 8 defines the value to be used for the provisioning timer. Sub-option 9 identifies FQDN for CMS to be used for primary line service, refer to RFC 2132 section 2 [7] for DHCP encoding and formatting details. Sub-option 10 defines parameters necessary for the AS-REQ/REP exchange backoff and retry mechanism of the Kerberized SNMPv3 key negotiation. Sub-option 11 defines parameters necessary for the AP-REQ/REP exchange backoff and retry mechanism of the Kerberized SNMPv3 key negotiation.

Option	Sub-option	Description and Comments
177	1	Service Provider's Primary DHCP Server Address
	2	Service Provider's Secondary DHCP Server Address
	3	Service Provider's SNMP Entity Address
	4	Service Provider Network Primary Domain Name Server
	5	Service Provider Network Secondary Domain Name Server
	6	SNMP Entity's Kerberos Realm Name of the Provisioning Realm
	7	Boolean, which when true, indicates the MTA should get its TGT
	8	Provisioning Timer
	9	FQDN of the CMS to be used for primary line service (E911/611
	10	Sub-option 10 defines parameters necessary for the AS-REQ/REP exchange backoff and retry mechanism of the Kerberized SNMPv3 key negotiation.
	11	Description and Comments: defines parameters necessary the AP-REP/REP exchange back off and retry mechanism of the Mercerized SNMPv3 key negotiation.

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 [7]. 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 [7] is assumed. For example, the standard DNS UDP port number is 42/udp.

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

The Service Provider's DHCP Server Addresses identify the DHCP servers that a DHCP OFFER will be accepted from in order to obtain an MTA-unique IP address for a given service provider's network administrative domain.

These addresses are configured as IPv4 addresses. If sub-option 1 contains the value 255.255.255.255 in lieu of a valid IP address, then the MTA MUST use logic defined in RFC 2131 to select an Offer. Otherwise, the MTA MUST only accept an Offer from the DHCP server(s) specified in sub-option(s) 1 and 2.

Sub-option 1 MUST be included in the DHCP OFFER to the CM and it indicates the Primary DHCP server IP address, a value of 255.255.255.255 or a value of 0.0.0.0. Sub-option 2 MAY be used to identify a redundant or backup DHCP server.

If both sub-options 1 and 2 contain a valid IP address then a DHCP Offer MAY be selected from the IP address in either sub. However, if the value in sub-option 2 is 255.255.255.255 then the value specified in sub-option 1 MUST take precedence over sub-option 2 and the MTA MUST retry exponentially for three attempts (e.g. 2, 4, 8 second intervals) before reverting to the value in sub-option 2. If the value specified in sub-option 1 is 255.255.255.255 then the value in sub-option 2 MUST be ignored.

If the value of sub-option 1 is 0.0.0.0 then this implies that the MTA portion of the device MUST not attempt to provision The MTA MUST disregard sub-option 2 if the value of sub-option 1 is 0.0.0.0.

The encoding of sub-option 1 is as follows:

Option	Sub-option	Value	Comments
177	1	[xxx.xxx.xxx.xxx]:NNNN	The IP address of the Primary DHCP Server where NNNN is an optional UDP port number if different than the well-known port defined in [7].
177	2	[xxx.xxx.xxx.xxx]:NNNN	The IP address of the Secondary DHCP Server where NNNN is an optional UDP port number if different than the well-known port defined in [7].

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

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

A value of 0.0.0.0 in suboption 3 of a valid MTA DHCP OFFER specifies that the MTA MUST shutdown and not try to provision unless it is reinitialized by the CM. This is explained in step MTA2 of the provisioning flow process of Section 7.2.

This address MUST be configured as an FQDN.

Sub-option 3 MUST be included in the DHCP offer to the MTA. The encoding of sub-option 3 is as follows:

Option	Sub-option	Value	Comments
177	3	FQDN:NNNN	The FQDN of Service Provider's SNMP Entity, where NNNN is an optional UDP port number if different than the well-known port defined in [7].

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

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

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

Option	Sub-option	Value	Comments
177	4	[xxx.xxx.xxx.xxx]:NNNN	This field is the IPv4 address of the service provider's primary DNS server. Where NNNN is an optional UDP port number if different than the well-known port defined in [7].
177	5	[xxx.xxx.xxx.xxx]:NNNN	This field is the IPv4 address of the service provider's secondary DNS server. Where NNNN is an optional UDP port number if different than the well known port defined in [7].

8.1.3 Kerberos Realm of SNMP Entity (sub-option 6 and sub-option 7)

In conjunction with the SNMP Entity, the Kerberos Realm is used as a means of contacting a SNMP Entity in the provisioning realm. Sub-option 6 MUST and sub-option 7 MAY be included in the DHCP offer to the MTA.

Option	Sub-option	Value	Comments
177	6	KrbRealm	The Kerberos Realm Name of the SNMP Entity. The realm is used to perform a DNS SRV lookup for the KDC of the SNMP Entity.
177	7	GetTGT	Boolean, which when true, indicates the MTA SHOULD get its TGT.

8.1.3.1 SNMPv3 Key Establishment

The AP Request/AP Reply described in Figure 5, the accompanying flow description, and the security specification are used by the MTA in the initial provisioning phase to establish keys with the SNMPv3 USM User "MTA-Prov-xx:xx:xx:xx:xx:xx". Where xx:xx:xx:xx:xx:xx represents the MAC address of the MTA and MUST be uppercase. The MTA MUST instantiate this user in the USM MIB described in RFC 2574 [18] with the ability to be keyed using the PacketCable Kerberized key management method described in the security specification. SNMPv3 authentication is required and privacy is optional. For the list of allowed SNMPv3 authentication and privacy algorithms see [5].

Additionally, the usmUserSecurityName MUST be the set to the string "MTA-Prov-xx:xx:xx:xx:xx:xx" (quotation marks not included). Where xx:xx:xx:xx:xx:xx represents the MAC address of the MTA and MUST be uppercase. This ensures a unique usmUserSecurityName is created for each MTA.

The MTA must first obtain a service ticket for the provisioning realm as described in step MTA9. USM key management is performed over UDP, as specified in [5]. The SNMPv3 keys are established prior to any SNMPv3 communication and therefore SNMPv3 messages MUST be authenticated at all times (with privacy being optional). The MTA MUST use the USM user created above in the initial INFORM.

8.1.4 Provisioning Timer (sub-option 8)

Sub-option 8 defines the value to be used for the provisioning timer. This sub-option MAY be implemented if is desired to override the default value of the timer, which is specified by the pktcMtaDevProvisioningTimer object in the MTA MIB.

Option	Sub-Option	Value	Comments
177	8	NN	Value of the provisioning timer to be used to override the default, where NN represents an integer value between 0 and 30 minutes.

8.1.5 CMS for primary line service (sub-option 9)

In order to provide primary line service (E911/611), the CMS to be used for such service must be specified. By specifying the CMS in the DHCP options, it is available for E911/61 service following the completion of step MTA4.

DHCP option 177, suboption 9 MUST be included in the DHCP Offer if primary line service is enabled (E911/611). The encoding of suboption 9 is as follows:

Option	Sub-Option	Value	Comments
177	9	FQDN	The FQDN of the CMS to be used for E911/611 services before provisioning is completed.

8.1.6 AS-REQ/REP Exchange Backoff and Retry for SNMPv3 Key Management

AS-REQ/REP exchange backoff and retry mechanism of the Kerberized SNMPv3 key negotiation defined in [5] is controlled by the values delivered by "suboption-10" of the DHCP Option 177 or by the default values of the corresponding MIB objects in the Realm Table if "suboption-10" is not present in the DHCP Option 177.

An MTA MUST be able to retrieve the above parameters from suboption-10, if they are supplied by the Provisioning Server.

Provisioning Server MAY provision an MTA with the above parameters using suboption-10.

MTA MIB Object Name in pktcMtaDevRealmTable	Length (bytes)	Offset in Suboption-10	Comments
pktcMtaDevRealmUnsolicited KeyNomTimeout	4 (MSB first)	0	Defines the starting value of the timeout for the AS-REQ/REP Backoff and Retry mechanism with exponential timeout.
PktcMtaDevRealmUnsolicited KeyMaxTimeout	4 (MSB first)	4	Defines the Max. value of the timeout for the AS-REQ/REP Backoff and Retry mechanism with exponential timeout.
PktcMtaDevRealmUnsolicited KeyMaxRetries	4 (MSB first)	8	Defines the number of retries for the AS-REQ/REP Backoff and Retry mechanism.

If any of the values defined in the "suboption-10" is zero then the default value of the corresponding column from the Realm Table MUST be used.

8.1.7 AP-REQ/REP Kerberized Provisioning Backoff and Retry

AP-REQ/REP backoff and retry mechanism of the Kerberized SNMPv3 key negotiation defined in [5] is controlled by the values delivered by the "suboption-11" of the DHCP Option 177, and it uses the following MTA MIB Objects for the Timeouts in backoff and retry procedure:

"pktcMtaDevProvUnsolicitedKeyMaxTimeout"

"pktcMtaDevProvUnsolicitedKeyNomTimeout"

"pktcMtaDevProvUnsolicitedKeyMaxRetries"

An MTA MUST be able to retrieve the above parameters from suboption-11, if they are supplied by the Provisioning Server.

Provisioning Server MAY provision an MTA with the above parameters using suboption-11.

The following table defines the layout of the values in "suboption-11":

MTA MIB Object Name	Length (bytes)	Offset in Suboption-11	Comments
PktcMtaDevProvUnsolicitedKeyNomTimeout	4 (MSB first)	0	Defines the starting value of the timeout for the AP-REQ/REP Backoff and Retry mechanism with exponential timeout.
PktcMtaDevProvUnsolicitedKeyMaxTimeout	4 (MSB first)	4	Defines the Max. value of the timeout for the AP-REQ/REP Backoff and Retry mechanism with exponential timeout.
PktcMtaDevProvUnsolicitedKeyMaxRetries	4 (MSB first)	8	Defines the number of retries for the AP-REQ/REP Backoff and Retry mechanism.

8.2 Code 60: Vendor Client Identifier

Option code 60 contains a string identifying Capabilities of the MTA. The MTA- MUST send the following ASCII Coded String in DHCP Option code 60: "pktc1.0:xxxxxx". Where xxxxxx MUST be an ASCII representation of the hexadecimal encoding of the MTA TLV Encoded Capabilities, as defined in Section 10.

8.3 DHCP Options 12 and 15

MTA FQDN MUST be sent to the E-MTA in Option-12 and Option-15. Option-12 MUST contain "Host Name" part of the FQDN, and the Option-15 MUST contain "Domain Name" part of the FQDN.

For example, if MTA FQDN is "mta1.pclab.com", then Option-12 must contain "mta1" and Option-15 must contain "pclab.com".

9 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 SNMPv3 security.

PacketCable 1.0 requires that a MTA configuration data file MUST be provided to all embedded-MTAs during the registration sequence. Endpoint voice services do not have to be enabled at the time of initialization. MTA device level configuration data MUST be provisioned during initialization. These items are contained in section 9.1.1.

The MTA configuration data URL 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.

9.1 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 or PacketCable type 64. TLV 64 is a PacketCable defined TLV where the length value is 2 bytes long instead of the 1 byte for DOCSIS TLV type 11. The TLV type 64 MUST be used when the length is greater than 254 bytes. If desired, vendor-specific information may be added to the configuration file using the vendor-specific TLV43. This TLV has been specified by the DOCSIS [6]. Vendors MUST never provision vendor-specific information using TLV type 11 or 64.

Type	Length	Value
11	n, where n is 1 byte	variable binding
64	m, where m is 2 bytes	variable binding
NOTE: Provisioning SHOULD use type 11 where possible		

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 attributes identified as "required" in the Device Level Configuration Data table, which appears in section 9.1.1. The MTA configuration file MAY contain any of the non-required attributes which appear in the Device Level Configuration Data table. If the configuration file does not contain required attributes, it MUST be rejected. The MTA configuration file MUST be sent to the embedded-MTA every time this device is powered on. The MTA enrollment inform (step MTA15 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. 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 using SNMPv3 security. Refer to section 7.4.1 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 Per-Endpoint Configuration Data table, which appears in section 9.1.3. The MTA configuration file MAY contain any of the non-required attributes which appear in the Per-Endpoint Configuration Data table 7. 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 7.4.1 for a discussion concerning synchronization of provisioning attributes with back office systems.

The MTA Configuration File MUST contain Per-Realm Configuration Data. Per-Realm Configuration Data MUST contain at least the data for the Provisioning Realm that is identified in DHCP Option-177, Suboption-6.

After Receiving the MTA Configuration File, an MTA MUST validate the following:

- "pktcMtaDevRealmName" MIB Object of the Realm Table MUST be the same as the Realm Name supplied to the MTA in DHCP Option-177, Suboption-6.
- "pktcMtaDevRealmOrgName" MIB Object of the Realm Table MUST be the same as the "Organization Name" attribute in the Service Provider Certificate.
- Encryption and Authentication of the MTA Configuration File as per [5].

An MTA MUST treat any of the above validation failures as failure of the MTA23 Provisioning Flow and the MTA MUST discard the Configuration File

If the value of any attribute identified as "required" is incorrect the MTA MUST reject the configuration file. If the value of any attribute identified as "optional" is incorrect the MTA MUST assign that attribute its default value and continue to process the configuration file.

If the MTA encounters a vendor-specific TLV43 with a vendor ID that the MTA does not recognize as it's own the MTA must ignore the TLV 43 and the MTA MUST continue to process the configuration file. If the MTA detects the presence on any TLV other than TLV 11, TLV 43 TLV 64, or TLV254 it MUST reject the configuration file. If the MTA encounters an unrecognized variable binding in a TLV 11 or TLV 64 it MUST reject the configuration file.

9.1.1 Device Level Configuration Data

Refer to the MTA MIB [2] for more detailed information concerning these attributes and their default values.

- The MTA Manufacturer Certificate validates the MTA Device Certificate.

Attribute	Syntax	Configuration Access	SNMP Access	MIB File	Object	Comments
Telephony Config File Start	Integer	W, required	None	N/A	N/A	Type length value 254 1 1 The MTA config file MUST start with this attribute.
Telephony Config File End	Integer	W, required	None	N/A	N/A	Type length value 254 1 255 This MUST be the last attribute in the MTA config file.
Telephony MTA Admin State	ENUM	W, required	R/W	MTA Device MIB	pktcMtaDevEnabled	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.
Solicited Key Timeout	Integer	W, optional	R/W	N/A	pktcMtaDevProvSolicitedKeyTimeout	This timeout applies only when the Provisioning Server initiated key management (with a Wake Up message) for SNMPv3. It is the period during which the MTA will save a nonce (inside the sequence number field) from the sent out AP Request and wait for the matching AP Reply from the Provisioning Server. Since there is a default value, this is optional.

9.1.2 Device Level Service Data

Refer to the MTA MIB [2], the SIGNALING MIB [3], the NCS Call Signaling specification [4] and RFC 2475 [25] for more detailed information concerning these attributes and their default values.

Attribute	Syntax	Configuration Access	SNMP Access	MIB File	Object	pktcDevEvSysloComments
NCS Default Call Signaling TOS	Integer	W, optional	R/W	MTA Signaling MIB	pktcSigDefCallSigTos	The default value used in the IP header for setting the TOS value for NCS call signaling.
NCS Default Media Stream TOS	Integer	W, optional	R/W	MTA Signaling MIB	pktcSigDefMediaStreamTos	The default value used in the IP header for setting the TOS value for NCS media stream packets.
MTA UDP receive port used for NCS	Integer (1025..65 535)	W, optional	R/O	MTA Signaling MIB	pktcSigDefNcsReceiveUdpPort	This object contains the MTA User Datagram Protocol Receive Port that is used for NCS call signaling. This object should only be changed by the configuration file.
NCS TOS Format Selector	ENUM	W, optional	R/W	MTA Signaling MIB	pktcSigTosFormatSelector	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, optional	R/W	MTA Signaling MIB	pktcSigDevR0Cadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000

Attribute	Syntax	Configuration Access	SNMP Access	MIB File	Object	pktcDevEvSysloComments
R6 cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevR6Cadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000
R7 cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevR7Cadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000
R1 cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevR1Cadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000

Attribute	Syntax	Configuration Access	SNMP Access	MIB File	Object	pktcDevEvSysloComments
R2 cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevR2Cadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000
R3 cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevR3Cadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000
R4 cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevR4Cadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000

Attribute	Syntax	Configuration Access	SNMP Access	MIB File	Object	pktcDevEvSysloComments
R5 cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevR5Cadence	User defined field where each bit (least significant bit) represents a duration of 100 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000
Rg cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevRgCadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000
Rt cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevRtCadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds (6 seconds total) 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000

Attribute	Syntax	Configuration Access	SNMP Access	MIB File	Object	pktcDevEvSysloComments
Rs cadence	Bit-field	W, optional	R/W	MTA Signaling MIB	pktcSigDevRsCadence	User defined field where each bit (least significant bit) represents a duration of 100 milliseconds 1= active ringing, 0= silence 64 bits are used for representation; MSB 60 bits for ring cadence. Bit 61 is used to represent repeatable(when set to ZERO) and non repeatable(when set to ONE). Other three bits are reserved for future use, and currently set to 000.
Call Signaling SCN Up	String	W	R/W	MTA Signaling MIB	pktcSigServiceClassNameUS	The string contains the Service Class Name that is to be used when the Service Flow is created for the upstream direction.
Call Signaling SCN Down	String	W	R/W	MTA Signaling MIB	pktcSigServiceClassNameDS	The string contains the Service Class Name that is to be used when the Service Flow is created for the downstream direction.
Call Signaling Network Mask	Integer32	W	R/W	MTA Signaling MIB	pktcSigServiceClassNameMask	The value is used as the NCS Call Signaling classifier mask.

9.1.3 Per-Endpoint Configuration Data

Refer to the SIGNALING MIB [3], the NCS spec [4], the security spec [5] and the MTA MIB [2] for more detailed information concerning these attributes and their default values.

MTA sends KDC the MTA/CMS certificate, MTA's FQDN, CMS-ID. The KDC returns the MTA a "Kerberos Ticket" that says "this MTA is assigned to this CMS"

The Telephony Service Provider Certificate validates the MTA Telephony Certificate

If two different endpoints share the same Kerberos Realm and same CMS FQDN, then these four attributes MUST be identical: PKINIT grace period, KDC name list, MTA telephony certificate, telephony service provider certificate.

Attribute	Syntax	Access	SNMP Access	MIB File	Object	Comments
Port Admin State	ENUM	W, optional	R/W	IF-MIB (RFC 2863)	ifAdminStatus	The administrative state of the port the operator can access to either enable or disable service to the port. The administrative state can be used to disable access to the user port without de-provisioning the subscriber. Allowed values for this attribute are: up(1) or down(2). For SNMP access ifAdminStatus is found in the ifTable of MIB-II.
Call Management Server Name	String	W, required	R/W	MTA Signaling MIB	pktcNcsEndPntConfigCallAgentId	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	MTA Signaling MIB	pktcNcsEndPntConfigCallAgentUdpPort	UDP port for the CMS.
Partial Dial Timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigPartialDialTO	Timeout value in seconds for partial dial timeout.
Critical Dial Timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigCriticalDialTO	Timeout value in seconds for critical dial timeout.
Busy Tone Timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigBusyToneTO	Timeout value in seconds for busy tone.
Dial tone timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigDialToneTO	Timeout value in seconds for dialtone.
Message Waiting timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigMessageWaitingTO	Timeout value in seconds for message waiting.
Off Hook Warning timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigOffHookWarnToneTO	Timeout value in seconds for off hook warning.

Attribute	Syntax	Access	SNMP Access	MIB File	Object	Comments
Ringing Timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigRingingTO	Timeout value in seconds for ringing.
Ringback Timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigRingBackTO	Timeout value in seconds for ringback.
Reorder Tone timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigReorderToneTO	Timeout value in seconds for reorder tone.
Stutter dial timeout	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigStutterDialToneTO	Timeout value in seconds for stutter dial tone.
TS Max	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigTSMax	Contains the maximum time in seconds since the sending of the initial datagram.
Max1	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigMax1	The suspicious error threshold for each endpoint retransmission.
Max2	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigMax2	The disconnect error threshold per endpoint retransmission.
Max1 Queue Enable	Enum	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigMax1QEnable	Enables/disables the Max1 DNS query operation when Max1 expires.
Max2 Queue Enable	Enum	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigMax2QEnable	Enables/disables the Max2 DNS query operation when Max2 expires.
MWD	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigMWD	Number of seconds to wait to restart after a restart is received.
Tdinit	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigTdinit	Number of seconds to wait after a disconnect.
TDMin	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigTdmin	Minimum number of seconds to wait after a disconnect.

Attribute	Syntax	Access	SNMP Access	MIB File	Object	Comments
TDMax	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigTdmax	Maximum number of seconds to wait after a disconnect.
RTO Max	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigRtoMax	Maximum number of seconds for the retransmission timer.
RTO Init	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigRtoInit	Initial value for the retransmission timer.
Long Duration Keepalive	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigLongDurationKeepAlive	Timeout in minutes for sending long duration call notification messages.
Thist	Integer	W	R/W	MTA Signaling MIB	pktcNcsEndPntConfigThist	The timeout period in seconds before no response is declared.
Call Waiting Max Reps	Integer	W, optional	R/W	MTA Signaling MIB	pktcNcsEndPntConfigCallWaitingMaxRep	This object contains the maximum number of repetitions of the call waiting that the MTA will play from a single CMS request. A value of zero (0) will be used when the CMS invokes any play repetition
Call Waiting Delay	Integer	W, optional	R/W	IF-MIB (RFC 2863)	pktcNcsEndPntConfigCallWaitingDelay	This object contains the delay between repetitions of the call waiting that the MTA will play from a single CMS request

9.1.4 Per-Realm Configuration Data

Refer to the MTA MIB [2] for more detailed information concerning these attributes and their default values. Refer to the security spec [5] for more information on the use of Kerberos realms. There MUST be at least one conceptual row in the pktcMtaDevRealmTable to establish service upon completion of configuration. These configuration parameters are optional in the config file, but if included the config file MUST contain at least one Realm name to permit proper instantiation of the table. There may be more than one set of entries if multiple realms are supported.

Attribute	Syntax	Access	SNMP Access	MIB File	Object	Comments
Pkinit Grace Period	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevRealmPkinitGracePeriod	For the purpose of IPSec key management with a CMS, the MTA MUST obtain a new Kerberos ticket (with a PKINIT exchange) this many minutes before the old ticket expires. The minimum allowable value is 15 mins. The default is 30 mins. This parameter MAY also be used with other Kerberized applications.
TGS Grace Period	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevRealmTgsGracePeriod	When the MTA implementation uses TGS Request/TGS Reply Kerberos messages for the purpose of IPSec key management with the CMS, the MTA MUST obtain a new service ticket for the CMS (with a TGS request) this many minutes before the old ticket expires. The minimum allowable value is 1 min. The default is 10 mins. This parameter MAY also be used with other Kerberized applications.
Realm Org Name	Integer	W, required	R/W	MTA Device MIB	pktcMtaDevRealmOrgName	The value of the X.500 organization name attribute in the subject name of the Service provider certificate.
Unsolicited Keying max Timeout	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevRealmUnsolicitedKeyMaxTimeout	This timeout applies only when the MTA initiated key management. The maximum timeout is the value which may not be exceeded in the exponential backoff algorithm.
Unsolicited Keying Nominal Timeout	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevRealmUnsolicitedKeyNomTimeout	This timeout applies only when the MTA initiated key management. Typically this is the average roundtrip time between the MTA and the KDC.
Unsolicited Keying Max Retries	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevRealmUnsolicitedKeyMaxRetries	This is the maximum number of retries before the MTA gives up attempting to establish a Security Association.

9.1.5 Per-CMS Configuration Data

Refer to the MTA MIB [2] for more detailed information concerning these attributes and their default values. There MUST be at least one conceptual row in the pktcDevCmsTable to establish service upon completion of configuration. These configuration parameters are optional in the config file, but if included the config file MUST identify at least one CMS and its corresponding Kerberos Realm Name. There may be more than one set of entries if multiple CMSs are supported.

As per Security Specification Requirement[5], the IPSEC signaling security must be controlled by the Operator depending on the deployment and operational conditions. As the IPSEC Security Association is established between the MTA and the CMS, the IPSEC enabling/disabling control should also be on per CMS basis. Enabling/Disabling of the IPSEC Signaling Security MUST be defined only by the information in the MTA's Configuration File when the file is being downloaded , and the enable/disable toggling MUST be done only as a result of the MTA Reset.

For more details on the MIB Object controlling the IPSEC enabling/disabling, refer to the MTA MIB [2].

Attribute	Syntax	Access	SNMP Access	MIB File	Object	Comments
Kerberos Realm Name	String	W, optional	R/W	MTA Device MIB	pktcMtaDevCmsKerbRealmName	The name for the associated Kerberos Realm. This is the corresponding Kerberos Realm Name in the Per Realm Configuration Data.
CMS Maximum Clock Skew	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevCmsMaxClockSkew	This is the maximum allowable clock skew between the MTA and CMS.
CMS Solicited Key Timeout	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevCmsSolicitedKeyTimeout	This timeout applies only when the CMS initiated key management (with a Wake Up or Rekey message). It is the period during which the MTA will save a nonce (inside the sequence number field) from the sent out AP Request and wait for the matching AP Reply from the CMS.
Unsolicited Key Max Timeout	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevCmsUnsolicitedKeyMaxTimeout	This timeout applies only when the MTA initiated key management. The maximum timeout is the value which may not be exceeded in the exponential backoff algorithm.
Unsolicited Key Nominal Timeout	Integer	W. optional	R/W	MTA Device MIB	pktcMtaDevCmsUnsolicitedKeyNomTimeout	This timeout applies only when the MTA initiated key management. Typically this is the average roundtrip time between the MTA and the CMS.
Unsolicited Key Max Retries	Integer	W, optional	R/W	MTA Device MIB	pktcMtaDevCmsUnsolicitedKeyMaxRetries	This is the maximum number of retries before the MTA gives up attempting to establish a security association.
IPSEC Control	Integer	W, optional	R/O	MTA Device MIB	pktcMtaDevCmsIpsecCtrl	IPSEC Control for each CMS: controls the IPSEC establishment and IPSEC related Key Management.

10 MTA DEVICE CAPABILITIES

MTA Capabilities string is supplied to the Provisioning Server in Option code 60 (Vendor Class Identifier) — to allow the Back-Office to differentiate between MTAs during the Provisioning Process. Use of Capabilities information by the Provisioning Application is optional.

Capabilities string is encoded as an ASCII string containing the Capabilities information in Type/Length/Value (TLV) Format.

For example, the ASCII encoding of the first two TLVs (PacketCable Version 1.0 and Number of Telephony Endpoints = 2) of an MTA would be 05nn010100020102. Note that many more TLVs are required for PacketCable MTA, and the field "nn" will contain the length of all the TLVs. This example shows only two TLVs for simplicity.

The "value" field describes the capabilities of a particular modem, i.e. implementation dependent limits on the particular features or number of features, which the modem can support. It is composed from a number of encapsulated TLV fields. The encapsulated sub-types define the specific capabilities for the MTA. Note that the sub-type fields defined are only valid within the encapsulated capabilities configuration setting string.

Type	Length	Value
5	n	

The set of possible encapsulated fields is described below.

MTA MUST Send Capabilities String in option 60 of the DHCP DISCOVER request.

10.1 PacketCable Version

This TLV MUST be supplied in the Capabilities String.

Type	Length	Values	Comment	Default Value
5.1	1	0	PacketCable 1.0	NONE
		1	PacketCable 1.1	
		2	PacketCable 1.2	
		3	PacketCable 1.3 (S-MTA)	
		4-255	Reserved	

10.2 Number Of Telephony Endpoints

This TLV MUST be supplied in the Capabilities String.

Type	Length	Values	Comment	Default
5.2	1	n	Number of endpoints	NONE

10.3 TGT Support

Type	Length	Value	Comment	Default Value
5.3	1	0	0: No	0
		1	1: Yes	

10.4 HTTP Download File Access Method Support

Type	Length	Value	Comment	Default Value
5.4	1	0	0: No	0
		1	1: Yes	

10.5 MTA-24 Event SYSLOG Notification Support

Type	Length	Value	Comment	Default Value
5.5	1	0	0: No	0
		1	1: Yes	

10.6 NCS Service Flow Support

Type	Length	Value	Comment	Default Value
5.6	1	0	0: No	0
		1	1: Yes	

10.7 Primary Line Support

Type	Length	Value	Comment	Default Value
5.7	1	0	0: No	0
		1	1: Yes	

10.8 Vendor Specific TLV Type(s)

This TLV can be supplied in the Capabilities String if an MTA requires a specific processing of the Vendor Specific TLV Type(s).

Type	Length	Value	Comment	Default Value
5.8	n	{seq-of-bytes}:	One type per byte	43
			per byte	

10.9 NVRAM Ticket/Session Keys Storage Support

Type	Length	Value	Comment	Default Value
5.9	1	0	0: No	0
		1	1: Yes	

10.10 Provisioning Event Reporting Support (para 5.4.3)

Type	Length	Value	Comment	Default Value
5.10	1	0	0: No	0
		1	1: Yes	

10.11 Supported CODEC(s)

This TLV MUST be supplied in the Capabilities String.

Type	Length	Value	Comment	Default Value
5.11	n	{seq-of-bytes}	one ID per byte	NONE

CODEC ID is the value represented by the Enumerated Type of "PktcCodecType" TEXTUAL CONVENTION in MTA MIB:

1: other,

2: unknown,

3: G.729,

4: reserved,

5: G.729E,

6: PCMU,

7: G.726-32

8: G.728,

9: PCMA,

10: G.726-16

11: G.726 24

12: G.726 40

10.12 Silence Suppression Support

Type	Length	Value	Comment	Default Value
5.12	1	0	0: No	0
		1	1: Yes	

10.13 Echo Cancellation Support

Type	Length	Value	Comment	Default Value
5.13	1	0	0: No	0
		1	1: Yes	

10.14 RSVP Support

Type	Length	Value	Comment	Default Value
5.14	1	0	0: No	0
		1	1: Yes	

10.15 UGS-AD Support

Type	Length	Value	Comment	Default Value
5.15	1	0	0: No	0
		1	1: Yes	

10.16 MTA's "ifIndex" starting number in "ifTable"

This TLV contains the value of the "ifIndex" for the first MTA Telephony Interface in "ifTable" MIB Table. The TLV MUST be supplied in the Capabilities String.

Type	Length	Value	Comment	Default Value
5.16	1	n	first MTA Interface	NONE

10.17 Provisioning Flow Logging Support

This capability is set to a corresponding value depending on the support of the logging capability of the Provisioning Flow (as per section 5.4.3).

Type	Length	Value	Comment	Default Value
5.17	1	0	0: No	0
		1	1: Yes	

Appendix I Provisioning Events

Event Name	Default Severity for Event	Default Display String	Comments
PROV-EV-1	Critical	"Waiting For DHCP Offer"	DHCP Discover has been transmitted and no offer has yet been received.
PROV-EV-2	Critical	"Waiting For DHCP Ack Response"	DHCP Request has been transmitted and no response has yet been received.
PROV-EV-3	Critical	"Waiting For ProvRealmKdcName Response"	DNS Srv request has been transmitted and no reply has yet been received.
PROV-EV-4	Critical	"Waiting For ProvRealmKdcAddr Response"	DNS Request has been transmitted and no reply has yet been received.
PROV-EV-5	Critical	"Waiting For AS-Reply"	AS request has been sent, and no MSO KDC AS Kerberos ticket reply has yet been received.
PROV-EV-6	Major	"Waiting For TGS-Reply"	TGS request has been transmitted and no TGS ticket reply has yet been received.
PROV-EV-7	Critical	"Waiting For AP-Reply"	AP request has been transmitted and no SNMPv3 key info reply has yet been received.
PROV-EV-8	Critical	"Waiting For Snmp GetRequest"	INFORM message has been transmitted and the device is waiting on optional/iterative GET requests.
PROV-EV-9	Critical	"Waiting For Snmp SetInfo"	MTA is waiting on config file download access information.
PROV-EV-10	Major	"Waiting For TFTP AddrResponse"	DNS Request has been transmitted and no reply has yet been received.
PROV-EV-11	Critical	"Waiting For ConfigFile"	TFTP request has been transmitted and no reply has yet been received or a download is in progress.
PROV-EV-12	Major	"Waiting For TelRealmKdc NameResponse"	DNS Srv request has been transmitted and no name reply has yet been received.
PROV-EV-13	Major	"Waiting For TelRealmKdc Addr Response"	DNS Request has been transmitted and no address reply has yet been received.
PROV-EV-14	Major	"Waiting For Pkinit AS-Reply"	AS request has been transmitted and no ticket reply has yet been received.
PROV-EV-15	Major	"Waiting For CmsKerbTick TGS-Reply"	TGS request has been transmitted and no ticket reply has yet been received.
PROV-EV-16	Major	"Waiting For CmsKerbTick AP-Reply"	AP request has been transmitted and no Ipsec parameters reply has yet been received.
PROV-EV-17	Critical	"Provisioning TimeOut"	the provisioning sequence took too long from MTA15 to MTA19(specified in pktcMtaDevProvisioningTimer).

Event Name	Default Severity for Event	Default Display String	Comments
PROV-EV-18	Critical	"ConfigFile – BadAuthentication"	the config file authentication value did not agree with the value inpktcMtaDevProvConfigHash or the authentication parameters were invalid.
PROV-EV-19	Critical	"ConfigFile – BadPrivacy"	the privacy parameters were invalid.
PROV-EV-20	Critical	"ConfigFile – BadFormat"	the format of the configuration file was not as expected.
PROV-EV-21	Major	"ConfigFile – MissingParam"	mandatory parameter of the configuration file is missing.
PROV-EV-22	Major	"ConfigFile – BadParam"	parameter within the configuration file had a bad value.
PROV-EV-23	Major	"ConfigFile – BadLinkage"	table linkages in the configuration file could not be resolved.

Appendix II 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:

Sumanth Channabasappa (Alopa Networks)

Angela Lyda, Rick Morris, Rodney Osborne (Arris Interactive);

Steven Bellovin and Chris Melle (AT&T);

Eugene Nechamkin (Broadcom);

John Berg, Maria Stachelek (CableLabs);

Klaus Hermanns, Azita Kia, Michael Thomas, Rich Woundy (Cisco);

Deepak Patil (Com21);

Jeff Ollis, Rick Vetter (General Instrument/Motorola);

Roger Loots, David Walters (Lucent);

Burcak Besar (Pacific Broadband);

Peter Bates (Telcordia);

Patrick Meehan (Tellabs);

Satish Kumar, Itay Sherman and Roy Spitzer (Texas Instrument),

Aviv Goren (Terayon);

Prithivraj Narayanan (Wipro)

A special thanks is due to Angela Lyda (Arris), Rick Vetter (Motorola), and Roy Spitzer (Telogy) who worked tirelessly in a challenging multi-vendor environment to build this specification.

Matt Osman, CableLabs

Appendix III Revisions

Engineering Change Numbers incorporated in PKT-SP-I02-010323.

ECN	ECN Date	Summary
prov-n-00008	4/20/00	MTA Device Signature
prov-n-99005-v2	4/28/00	MTA's two separate code images
prov-n-00023	6/2/00	Telephony Certificate
prov-n-00024-v2	6/2/00	Security Association
prov-n-00030-v2	6/9/00	DHCP options
sec-n-00022-v2	6/2/00	TGS Certificate
mib-n-00027	6/9/00	Configuration file entities
prov-n-00026	9/11/00	New TLV
prov-n-00043-v3	9/11/00	Provisioning flow sequencing
prov-n-00019-v3	9/25/00	DHCP option code 60
prov-n-00099	1/15/01	Examples for HTTP and TFTP transport protocols
prov-n-00101	1/15/01	Provisioning Correlation ID
prov-n-00100-v2	1/22/01	Clarification
prov-n-00122	1/22/01	TLV value is now specified
sec-n-00146-v214	1/22/01	Secure Provisioning ECN
sec-n-00079	3/12/01	Kerberos principal name without downloading new config file
prov-n-00098-v3	3/5/01	Behavior of MTA for changed DHCP values
prov-n-01006	2/26/01	X.509 Certificate
prov-n-01008-v3	3/5/01	Encryption keys for SNMPv3 Informs
prov-n-01012	3/12/01	DHCP information in the config file
prov-n-01013	3/12/01	Clarify previous ECNs impact
prov-n-01018	3/26/01	MIB changes impact on I02
prov-n-01017	3/12/01	MTA and SNMP set

Engineering Change incorporated in PKT-SP-I03-011221.

ECN ID	ECN Date	Summary
mib-n-01077	7/16/01	Clarify usage of pktcMtaDev Provisioning Timer, clean up some security related objects
prov-n-01033-v2	5/7/01	Error conditions that can occur between MTA15 and MTA25.
prov-n-01037	5/7/01	Several editorial changes in Security document.
prov-n-01038	5/7/01	It is not clear what event is reported if an endpoint is provisioned or an endpoint is no longer provisioned.
prov-n-01039	5/7/01	Config file MUST be rejected if the required info is not present.
prov-n-01059	6/4/01	Language clarification regarding the Provisioning Flow as a mandatory requirement.
prov-n-01060	6/4/01	Testing group cannot easily determine associated MIB object used in configuration file
prov-n-01061	6/4/01	The receive UDP port cannot be configured using the config file.
prov-n-01065	6/4/01	Revise wording in section 9.1 to specify the tables being referenced.
prov-n-01066	6/18/01	Correct typos in ECN 00184
prov-n-01076	7/16/01	Clarification regarding the presence of the "Telephony Service Provider SNMP Entity" attribute in the Device Level Configuration Data.
prov-n-01078	7/16/01	Clarify the intent of the e-MTA firmware download
prov-n-01079	7/16/01	The Provisioning Specification (I02) allows two ways of distributing of the MTA FQDN
prov-n-01106	8/20/01	Duplicate instances of requirement statements for Code 177 sub-option 1 thru 7 are deleted. Also corrects typo.
prov-n-01118-v2	9/10/01	The description of the requirements for tables (and their corresponding MIB entries) is unclear.
prov-n-01119	9/10/01	Augment sec-n-01029 and clear up several.
prov-n-01123	9/10/01	MTA Provisioning Spec clarification on MTA FQDN supply to E-MTA during provisioning.
prov-n-01156	10/15/01	Add suboption 9 to DHCP option 177 to support provisioning CMS for E911/611 service.
prov-n-01157	10/15/01	Clarification in the usage of "pktcSigDefNcsReceiveUdpPort" MIB object.
prov-n-01176	11/19/01	Additions on the usage of the Log Event Mechanism in E-MTA
prov-n-01198	11/19/01	Add "MUST" statements to provisioning flows MTA20 – MTA22
prov-n-01182	12/10/01	Provisioning of the Signaling Communication Path between the MTA and CMS introduced, with new conf file TLV.
prov-n-01219	12/17/01	Correction of minor typographical errors and modifications to provisioning specification.

The following Engineering Change are incorporated in PKT-SP-PROV-I04-021018.

ECN ID	ECN Date	Summary
mibsig-n-02043	6/24/02	Changes representation of ring cadences to allow more granular ring cadences
prov-n-02014	6/24/02	While Provisioning Specification mandates Kereberized SNMPv3 key negotiation, it does not define the mechanism for initial delivery of the timeouts for the AS-REQ/REP backoff and retry mechanism.
prov-n-02020	6/24/02	Remove statements carried over from I01 version that are irrelevant now.
prov-n-02025	6/24/02	Allow and define how vendor-specific information should be entered in the MTA configuration file
prov-n-02026	6/24/02	Editorial Corrections and Clarifications
prov-n-02032	6/24/02	Insure that all DHCP ACK message content is treated as authoritative.
prov-n-02033	6/24/02	The behavior of the MTA during its provisioning MUST be dictated by the presence/ absence of option code 177 and if present, the value in its suboptions.
prov-n-02045	6/24/02	In Section 7.6, paragraph 1 it is not clear whether or not the NCS Service Flow MUST be implemented on the MTA.
prov-n-02050	6/24/02	Correction to the description of the Service Provider's SNMP Entity Address in section 8.1.2 to bring in line with the related pktcMtaDevSnmpEntity MIB definition in PKT-SP-MIB-MTA-I03-020116.
prov-n-02076	6/24/02	Specification requires clarification about MTA behavior under specific conditions for DHCP in regard to the use of option codes and PacketCable specific sub-options.
prov-n-02090	6/24/02	Per-Realm Configuration data should have “MUST” attribute to be able to provide the “OrgName” in the MTA Configuration File needed to verify the validity of the Organization Name attribute in the Service Provider Certificate.
prov-n-02100	6/24/02	The ECR defines the list and the representation of the MTA Capabilities in DHCP Option-60.
prov-n-02106	7/1/02	MTA18 provisioning step contains “SHOULD” terminology for normal flow sequencing which contradicts the “MUST” condition for configuration file hash.
prov-n-02144	7/29/02	The current spec does not clearly specify the TFT retry and backoff mechanism.
prov-n-02145	7/29/02	There is a need for the Telephony Service Provider to shut of the MTA if and when required using DHCP.
prov-n-02146	7/29/02	Clarify the TLV to be used for lengths of values greater than 254 in the TLV configuration file.
prov-n-02155	8/22/02	Defines the approach, which would allow the Service Providers to control the enabling/disabling of the signaling security (IPSEC) and Key Management flows associated with it.