

SCTE • ISBE[®]

S T A N D A R D S

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 165-05 2019

IPCablecom 1.5 Part 5: MTA Device Provisioning

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) / International Society of Broadband Experts (ISBE) Standards and Operational Practices (hereafter called “documents”) are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability, best practices and ultimately the long-term reliability of broadband communications facilities. These documents shall not in any way preclude any member or non-member of SCTE•ISBE from manufacturing or selling products not conforming to such documents, nor shall the existence of such standards preclude their voluntary use by those other than SCTE•ISBE members.

SCTE•ISBE assumes no obligations or liability whatsoever to any party who may adopt the documents. Such adopting party assumes all risks associated with adoption of these documents, and accepts full responsibility for any damage and/or claims arising from the adoption of such documents.

Attention is called to the possibility that implementation of this document may require the use of subject matter covered by patent rights. By publication of this document, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE•ISBE shall not be responsible for identifying patents for which a license may be required or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Patent holders who believe that they hold patents which are essential to the implementation of this document have been requested to provide information about those patents and any related licensing terms and conditions. Any such declarations made before or after publication of this document are available on the SCTE•ISBE web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2019
140 Philips Road
Exton, PA 19341

Note: DOCSIS® and PacketCable™ are registered trademarks of Cable Television Laboratories, Inc., and used in this document with permission.

Table of Contents

1	INTRODUCTION	9
1.1	PURPOSE	9
1.2	SCOPE	9
1.3	REQUIREMENTS AND CONVENTIONS	9
2	REFERENCES	10
2.1	NORMATIVE REFERENCES	10
2.2	INFORMATIVE REFERENCES	11
3	TERMS AND DEFINITIONS	13
4	ABBREVIATIONS AND ACRONYMS	17
5	BACKGROUND	24
5.1	SERVICE GOALS	24
5.2	SPECIFICATION GOALS	24
5.3	IP/CABLECOM REFERENCE ARCHITECTURE	25
5.4	COMPONENTS AND INTERFACES.....	26
5.4.1	MTA.....	27
5.4.2	Provisioning Server.....	28
5.4.3	MTA to Telephony Syslog Server.....	28
5.4.4	MTA to DHCP Server	28
5.4.5	MTA to Provisioning Application.....	28
5.4.6	MTA to CMS.....	29
5.4.7	MTA to Security Server (KDC).....	29
5.4.8	MTA and Configuration Data File Access.....	29
5.4.9	DOCSIS Extensions for MTA Provisioning.....	29
6	PROVISIONING OVERVIEW	31
6.1	DEVICE PROVISIONING.....	31
6.2	ENDPOINT PROVISIONING.....	31
6.3	SECURE FLOW PROVISIONING STATE TRANSITIONS	31
6.4	BASIC AND HYBRID FLOW PROVISIONING STATE TRANSITIONS	33
7	PROVISIONING FLOWS.....	34
7.1	BACKOFF, RETRIES, AND TIMEOUTS.....	34
7.2	EMBEDDED-MTA POWER-ON INITIALIZATION FLOW (SECURE FLOW)	35
7.2.1	Embedded-MTA Secure Power-on Initialization Flow (IPv4 eCM).....	36
7.2.2	Embedded-MTA Secure Power-on Initialization Flow (IPv6 eCM).....	43
7.3	EMBEDDED-MTA POWER-ON INITIALIZATION FLOW (BASIC FLOW).....	45
7.4	EMBEDDED-MTA POWER-ON INITIALIZATION FLOW (HYBRID FLOW)	47
7.5	ENDPOINT PROVISIONING COMPLETION NOTIFICATIONS	50
7.6	POST INITIALIZATION INCREMENTAL PROVISIONING	50
7.6.1	Synchronization of Provisioning Attributes with Configuration File	50
7.6.2	Adding/Enabling Telephony Services on an MTA Endpoint	51
7.6.3	Deleting/Disabling Telephony Services on an MTA Endpoint	52
7.6.4	Modifying Telephony Services on an MTA Endpoint.....	53
7.7	REFLECTING THE STATE OF THE ENDPOINT INTERFACE IN THE IFTABLE.	53
7.8	PROVISIONING OF THE SIGNALING COMMUNICATION PATH BETWEEN THE MTA AND CMS.....	54
7.9	MTA REPLACEMENT	54

7.10	TEMPORARY SIGNAL LOSS	54
7.11	MTA HARD REBOOT/SOFT RESET SCENARIOS.	54
8	DHCP OPTIONS	55
8.1	DHCP OPTION 122: CABLELABS CLIENT CONFIGURATION OPTION	55
8.1.1	Service Provider's DHCP Address (Sub-option 1 and 2)	56
8.1.2	Service Provider's Provisioning Entity Address (Sub-option 3)	57
8.1.3	AS-REQ/REP Exchange Backoff and Retry for SNMPv3 Key Management (Sub-option 4)	57
8.1.4	AP-REQ/REP Kerberized Provisioning Backoff and Retry (Sub-option 5)	57
8.1.5	Kerberos Realm of SNMP Entity (Sub-option 6)	58
8.1.6	Ticket Granting Server Usage (Sub-option 7)	58
8.1.7	Provisioning Timer (Sub-option 8)	59
8.1.8	Security Ticket Invalidation (Sub-option 9)	59
8.2	DHCP OPTION 60: VENDOR CLIENT IDENTIFIER	59
8.3	DHCP OPTIONS 12 AND 15	59
8.4	DHCP OPTION 6	59
8.5	DHCP OPTION 43	59
8.6	DHCP OPTION 1	61
8.7	DHCP OPTION 3	61
8.8	DHCP OPTION CL_V4_PACKETCABLE_MIB_ENV_OPTION	61
9	MTA PROVISIONABLE ATTRIBUTES	63
9.1	MTA CONFIGURATION FILE	63
9.1.1	Device Level Configuration Data	67
9.1.2	Device Level Service Data	68
9.1.3	Per-Endpoint Configuration Data	72
9.1.4	Per-Realm Configuration Data	75
9.1.5	Per-CMS Configuration Data	76
9.1.6	Exclusion of MIB Objects in Configuration File	78
10	MTA DEVICE CAPABILITIES	79
10.1	IPCABLECOM VERSION	79
10.2	NUMBER OF TELEPHONY ENDPOINTS	79
10.3	TGT SUPPORT	79
10.4	HTTP DOWNLOAD FILE ACCESS METHOD SUPPORT	79
10.5	MTA-24 EVENT SYSLOG NOTIFICATION SUPPORT	80
10.6	NCS SERVICE FLOW SUPPORT	80
10.7	PRIMARY LINE SUPPORT	80
10.8	VENDOR SPECIFIC TLV TYPE(S)	80
10.9	NVRAM TICKET/TICKET INFORMATION STORAGE SUPPORT	80
10.10	PROVISIONING EVENT REPORTING SUPPORT	80
10.11	SUPPORTED CODEC(S)	80
10.12	SILENCE SUPPRESSION SUPPORT	81
10.13	ECHO CANCELLATION SUPPORT	81
10.14	RSVP SUPPORT	81
10.15	UGS-AD SUPPORT	81
10.16	MTA's "IFINDEX" STARTING NUMBER IN "IFTABLE"	82
10.17	PROVISIONING FLOW LOGGING SUPPORT	82
10.18	SUPPORTED PROVISIONING FLOWS	82
10.19	T38 VERSION SUPPORT	82
10.20	T38 ERROR CORRECTION SUPPORT	83
10.21	RFC 2833 DTMF SUPPORT	83
10.22	VOICE METRICS SUPPORT	83

10.23	DEVICE MIB SUPPORT	83
10.23.1	Issuing Organization Assignments	84
10.23.2	Representing MIBs	84
10.23.3	Representing IETF MIBs	84
10.23.4	Example	85
10.24	MULTIPLE GRANTS PER INTERVAL SUPPORT	85
10.25	V.152 SUPPORT	85
11	TLV-38 SNMP NOTIFICATION RECEIVER SPECIFICATION	86
11.1	SUB-TLVs OF TLV-38	86
11.1.1	SNMP Notification Receiver IP Address	86
11.1.2	SNMP Notification Receiver UDP Port Number	86
11.1.3	SNMP Notification Receiver Type	86
11.1.4	SNMP Notification Receiver Timeout	87
11.1.5	SNMP Notification Receiver Retries	87
11.1.6	SNMP Notification Receiver Filtering Parameters	87
11.1.7	SNMPv3 Notification Receiver Security Name	88
11.2	MAPPING OF TLV FIELDS INTO SNMP TABLES	88
11.2.1	Mapping of TLV Fields into Created SNMP Table Rows	88
11.3	TLV 38 AND TLV 11 CONFIGURATION EXAMPLE	94
11.3.1	TLV-38 Example	94
11.3.2	Content of the SNMP Framework Tables After Processing of the Above Example TLV 38s	95
12	SNMPV2C MANAGEMENT REQUIREMENTS	99
12.1	SNMPV2C CO-EXISTENCE MODE TABLES CONTENT CREATED BY MTA AFTER MTA-4 FOR HYBRID AND BASIC FLOWS	99
12.2	SNMP DEFAULT ENTRIES FOR SNMPV2C ACCESS	100
13	SERVICE INTERRUPTION IMPACT REPORTING AND OTHER ENHANCED FEATURES SUPPORT	103
13.1	EDOCSIS REQUIREMENTS SUPPORT	103
13.1.1	Impact Analysis and Reporting Requirements	103
13.2	IPCABLECOM EXTENSION MIB	103
13.2.1	MTA MIB Extension	103
13.2.2	Signaling MIB Extension	103
13.3	BATTERY BACKUP MIBS	104
13.4	SYSLOG MIBS	104
13.5	FOREIGN POTENTIAL DETECTION	104
APPENDIX I	SNMPV2C CO-EXISTENCE CONFIGURATION EXAMPLE - TEMPLATE FOR SERVICE PROVIDERS	105

List of Figures

FIGURE 1. TRANSPARENT IP TRAFFIC THROUGH THE DATA-OVER-CABLE SYSTEM	24
FIGURE 2. IPCABLECOM 1.5 NETWORK COMPONENT REFERENCE MODEL	26
FIGURE 3. IPCABLECOM PROVISIONING INTERFACES	26
FIGURE 4. DEVICE STATES AND STATE TRANSITIONS FOR SECURE FLOW PROVISIONING	32
FIGURE 5. DEVICE STATES AND STATE TRANSITIONS FOR BASIC AND HYBRID FLOW PROVISIONING	33
FIGURE 6. EMBEDDED-MTA SECURE POWER-ON INITIALIZATION FLOW (IPv4 ECM)	36
FIGURE 7. ECM PROVISIONING IN IPV6 MODE	43
FIGURE 8. EMBEDDED-MTA BASIC POWER-ON INITIALIZATION FLOW	45
FIGURE 9. EMBEDDED-MTA HYBRID POWER-ON INITIALIZATION FLOW	47

List of Tables

TABLE 1. MTA DEVICE PROVISIONING FLOW SELECTION	58
TABLE 2. DHCP OPTION 43 SYNTAX	60
TABLE 3. SNMPNOTIFYTABLE	89
TABLE 4. SNMPTARGETADDRTABLE	89
TABLE 5. SNMPTARGETADDREXTTABLE	90
TABLE 6. SNMPTARGETPARAMSTABLE	90
TABLE 7. SNMPNOTIFYFILTERPROFILETABLE	91
TABLE 8. SNMPNOTIFYFILTERTABLE	91
TABLE 9. SNMPCOMMUNITYTABLE	91
TABLE 10. USMUSERTABLE	92
TABLE 11. VACMSECURITYTOGROUPTABLE	93
TABLE 12. VACMACCESSTABLE	93
TABLE 13. VACMVIEWTREEFAMILYTABLE	94
TABLE 14. EXAMPLE CONFIGURATION FILE ELEMENTS	95
TABLE 15. SNMPCOMMUNITYTABLE	95
TABLE 16. SNMPTARGETADDREXTTABLE	95
TABLE 17. USMUSERTABLE	96
TABLE 18. VACMCONTEXTTABLE	96
TABLE 19. VACMSECURITYTOGROUPTABLE	96
TABLE 20. VACMACCESSTABLE	96
TABLE 21. VACMVIEWTREEFAMILYTABLE	96
TABLE 22. SNMPNOTIFYTABLE	97
TABLE 23. SNMPTARGETADDRTABLE	97
TABLE 24. SNMPTARGETPARAMSTABLE	97
TABLE 25. SNMPNOTIFYFILTERPROFILETABLE	97
TABLE 26. SNMPNOTIFYFILTERTABLE	98
TABLE 27. SNMPCOMMUNITYTABLE CONTENT	99
TABLE 28. SNMPTARGETADDRTABLE CONTENT	100
TABLE 29. SNMPTARGETADDREXTTABLE CONTENT	100
TABLE 30. VACMSECURITYTOGROUPTABLE DEFAULT ENTRIES	100
TABLE 31. VACMACCESSTABLE DEFAULT ENTRIES	101
TABLE 32. VACMVIEWTREEFAMILYTABLE DEFAULT ENTRY	101
TABLE 33. SNMPTARGETPARAMSTABLE DEFAULT ENTRY	101
TABLE 34. SNMPNOTIFYTABLE DEFAULT ENTRY	102
TABLE 35. SNMPNOTIFYFILTERPROFILETABLE DEFAULT ENTRY	102

TABLE 36. SNMPNOTIFYFILTERTABLE DEFAULT ENTRY.....	102
TABLE 37. SNMPCOMMUNITYTABLE TEMPLATE FOR BASIC AND HYBRID FLOWS CONFIGURATION FILE	105
TABLE 38. SNMPTARGETADDRTABLE TEMPLATE FOR BASIC AND HYBRID FLOWS CONFIGURATION FILE.....	105
TABLE 39. SNMPTARGETADDRExtTABLE TEMPLATE FOR BASIC AND HYBRID FLOWS CONFIGURATION FILE	106

This page left blank intentionally.

1 INTRODUCTION

1.1 Purpose

This specification describes the IPCablecom 1.5 embedded-MTA device initialization and provisioning. This specification is issued to facilitate design and field-testing leading to 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 an IPCablecom 1.5 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 an IPCablecom 1.5 network configuration. This document defines the provisioning of MTA components of the embedded MTA device (unless stated otherwise).

1.3 Requirements and Conventions

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

"MUST"	This word means that the item is an absolute requirement of this specification.
"MUST NOT"	This phrase means that the item is an absolute prohibition of this specification.
"SHOULD"	This word means that there may exist valid reasons in particular circumstances to ignore this item, but the full implications should be understood and the case carefully weighed before choosing a different course.
"SHOULD NOT"	This phrase means that there may exist valid reasons in particular circumstances when the listed behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
"MAY"	This word means that this item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because it enhances the product, for example; another vendor may omit the same item.

Other text is descriptive or explanatory.

2 REFERENCES

The following documents contain provisions which, through reference in this text, constitute provisions of this standard. At the time of Subcommittee approval, the editions indicated were valid. All documents are subject to revision, and while parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below, they are reminded that newer editions of those documents might not be compatible with the referenced version.

2.1 Normative References

In order to claim compliance with this standard, it is necessary to conform to the following standards and other works as indicated, in addition to the other requirements of this standard. Intellectual property rights may be required to implement these references.

- [1] IETF RFC 2131, DHCP: Dynamic Host Configuration Protocol, March 1997.
- [2] ANSI/SCTE 165-07 2019, IPCablecom 1.5 Part 7: MTA MIB.
- [3] ANSI/SCTE 165-08 2019, IPCablecom 1.5 Part 8: Signaling MIB.
- [4] ANSI/SCTE 165-03 2016, IPCablecom 1.5 Part 3: Network-Based Call Signaling Protocol.
- [5] ANSI/SCTE 165-10 2009, IPCablecom 1.5 Part 10: Security.
- [6] ANSI/SCTE 23-01 2019, DOCSIS 1.1 Part 1: Radio Frequency Interface.
- [7] IETF RFC 3413/STD0062, Simple Network Management Protocol (SNMP) Applications, December 2002.
- [8] IETF RFC 3414/STD0062, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002.
- [9] IETF RFC 3415/STD0062, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), December 2002.
- [10] IETF RFC 3396, Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4), November 2002.
- [11] IETF RFC 2132, DHCP Options and BOOTP Vendor Extensions, S. March 1997.
- [12] ANSI/SCTE 107 2009, Embedded Cable Modem Devices.
- [13] ANSI/SCTE 165-15 2019, IPCablecom 1.5 Part 15: Management Event MIB Specification.
- [14] ANSI/SCTE 165-16 2016, IPCablecom 1.5 Part 16: Management Event Mechanism.
- [15] ANSI/SCTE 165-21 2016, IPCablecom 1.5 Part 21: Signaling Extension MIB Specification.
- [16] ANSI/SCTE 165-20 2019, IPCablecom 1.5 Part 20: MTA Extension MIB specification.
- [17] CableLabs Definition MIB Specification, <http://www.cablelabs.com/specification/cablelabs-definition-mib-specification/> , CL-SP-MIB-CLABDEF, Cable Television Laboratories, Inc.
- [18] CableLabs Battery Backup MIB Specification, <http://www.cablelabs.com/specification/cablelabs-battery-backup-mib-specification/> , CL-SP-MIB-BB, Cable Television Laboratories, Inc.
- [19] ANSI/SCTE 135-02 2013, DOCSIS 3.0 Part 2: MAC and Upper Layer Protocols.
- [20] CableLabs' DHCP Options Registry Specification, <http://www.cablelabs.com/specification/cablelabs-dhcp-options-registry-2/> , CL-SP-CANN-DHCP-Reg, Cable Television Laboratories, Inc.
- [21] IETF RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), July 2003.
- [22] IETF RFC 4682, E. Multimedia Terminal Adapter (MTA) Management Information Base for PacketCable- and IPCablecom-Compliant Devices, December 2006.

- [23] IETF RFC 5098, Network-Based Call Signaling (NCS) MIB for PacketCable and IPCom Multimedia Terminal Adapters (MTAs), February 2008.
- [24] IETF RFC 5428, Management Event Management Information Base (MIB) for PacketCable- and IPCom-Compliant Devices. April 2009.

2.2 Informative References

The following documents may provide valuable information to the reader but are not required when complying with this standard.

- [25] IETF RFC 3442, The Classless Static Route Option for Dynamic Host Configuration Protocol (DHCP) version 4, December 2002.
- [26] Protocol Numbers and Assignment Services, Internet Assigned Numbers Authority, <http://www.iana.org/numbers.html>
- [27] IETF RFC 1350/STD0033, The TFTP Protocol (Revision 2), MIT, July 1992.
- [28] IETF RFC 1034/STD0013, Domain Names—Concepts and Facilities, November 1987.
- [29] IETF RFC 1035, Domain Names—Implementation and Specifications, November 1987.
- [30] IETF RFC 1591, Domain Name System Structure and Delegation, March 1994.
- [31] IETF RFC 3495, DHCP Option for CableLabs Client Configuration, March 2003.
- [32] ANSI/SCTE 165-01 2019, IPCom 1.5 Part 1: Architecture Framework Technical Report.
- [33] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, CM-SP-CMCI-C01-081104, Cable Television Laboratories, Inc.
- [34] IETF RFC 3417/STD0062, Transport Mappings for the Simple Network Management Protocol (SNMP), December 2002.
- [35] IETF RFC 2579, Textual Conventions for SMIV2, April 1999.
- [36] IETF RFC 3410, Introduction and Applicability Statements for Internet-Standard Management Framework, December 2002.
- [37] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, December 2002.
- [38] IETF RFC 3412/STD0062, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), December 2002.
- [39] ANSI/SCTE 23-03 2017, DOCSIS 1.1 Part 3: Operations Support System Interface.
- [40] IETF RFC 2821, Simple Mail Transfer Protocol, April 2001.
- [41] IETF RFC 1123/STD0003, Braden, R., Requirements for Internet Hosts -- Application and Support, October 1989.
- [42] IETF RFC 2349, TFTP Timeout Interval and Transfer Size Options, May 1998.
- [43] IETF RFC 1945, HTTP 1.0, May 1996; IETF RFC-2068, HTTP 1.1, January 1997
- [44] IETF RFC 2475, An Architecture for Differentiated Services, December 1998.
- [45] ANSI/SCTE 165-02 2016, IPCom 1.5 Part 2: Audio/Video Codecs.
- [46] ANSI/SCTE 165-04 2019, IPCom 1.5 Part 4: Dynamic Quality-of-Service.
- [47] IETF RFC 3594, PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option, September 2003.
- [48] IETF RFC 2782, A DNS RR for specifying the location of services (DNS SRV), February 2000.

- [49] ANSI/SCTE 165-06 2018, IPCablecom 1.5 Part 6: MIBs Framework Specification.
- [50] IETF RFC 2616, Hypertext Transfer Protocol -- HTTP/1.1, June 1999.
- [51] IETF RFC 3617, Uniform Resource Identifier (URI) Scheme and Applicability Statement for the Trivial File Transfer Protocol (TFTP), October 2003.
- [52] IETF RFC 3584, Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework, August 2003.
- [53] IETF RFC 3611, RTP Control Protocol Extended Reports (RTCP XR), November, 2003.

3 TERMS AND DEFINITIONS

IPCablecom 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 IPCablecom 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 IPCablecom.
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 than 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 headend 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 (MCU).

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.k.a. DOCSIS-QoS "service flow") A unidirectional sequence of packets associated with a Service ID (SID) and a QoS. Multiple multimedia streams may be carried in a single DOCSIS 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 IP/Cablecom 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 IP/Cablecom network.
H.323	An ITU-T recommendation for transmitting and controlling audio and video information. The H.323 recommendation requires the use of the ITU-T H.225 and ITU-T 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 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 an IPCablecom subscriber out to a user on the PSTN.
On-Net Call	A communication placed by one customer to another customer entirely on the IPCablecom Network.
One-way Hash	A hash function that has an insignificant number of collisions upon output.
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 anyone other than 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 AND ACRONYMS

IPCablecom specifications use the following abbreviations.

AAA	Authentication, Authorization and Accounting.
AES	Advanced Encryption Standard. A block cipher, used to encrypt the media traffic in IPCablecom.
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 mode. 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 headend which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.
CMSS	Call Management Server Signaling.
Codec	COder-DECoder.

COPS	Common Open Policy Service protocol. Defined in RFC 2748.
CoS	Class of Service. The type 4 tuple of a DOCSIS configuration file.
CRCX	Create Connection.
CSR	Customer Service Representative.
DA	Directory Assistance.
DE	Default. This is a DiffServ Per Hop Behavior.
DES	Data Encryption Standard.
DF	Delivery Function.
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.
DSA	Dynamic Service Add.
DSC	Dynamic Service Change.
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.
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.
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated."
FEID	Financial Entity ID.
FGD	Feature Group D signaling.
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 2821 [40] for details.
GC	Gate Controller.
GTT	Global Title Translation.
HFC	Hybrid Fiber/Coaxial. An HFC system is a broadband bi-directional shared media transmission system using fiber trunks between the headend 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 [43] 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 Telecommunication Union.
ITU-T	International Telecommunication Union–Telecommunication 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.
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.
MDCX	Modify Connection.
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.
MF	Multi-Frequency.
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 IP-Cablecom and PSTN.

MGCP	Media Gateway Control Protocol. Protocol follow-on to SGCP. Refer to IETF 2705.
MGPI	Multiple Grants Per Interval.
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 headend 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, MTP 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 Address Translation. Layer 3 in the Open System Interconnection (OSI) architecture.
Network Layer	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 number (see LNP).
NTP	Network Time Protocol. An internet standard used for synchronizing clocks of elements distributed on an IP network.
NTSC	National Television Standards Committee. Defines the analog color television broadcast standard used today in North America.
OID	Object Identification.
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.
PCES	IPCablecom Electronic Surveillance.
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.
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 2865 and RFC 2866) 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 IPCom.
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.
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. SFIDs are considered to be in either the upstream direction (USFID) or downstream direction (DSFID). Upstream Service Flow IDs and Downstream Service Flow IDs are allocated from the same SFID number space.
SFR	Service Flow Reference. A 16-bit message element used within the DOCSIS TLV parameters of Configuration Files and Dynamic Service messages to temporarily identify a defined Service Flow. The CMTS assigns a permanent SFID to each SFR of a message.
SG	Signaling Gateway. An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network. In particular, the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.
SGCP	Simple Gateway Control Protocol. Earlier draft of MGCP.
SHA – 1	Secure Hash Algorithm 1. A one-way hash algorithm.
SID	Service ID. A 14-bit number assigned by a CMTS to identify an upstream virtual circuit. Each SID separately requests and is granted the right to use upstream bandwidth.
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.
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 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. This is shown in simplified form in Figure 1. It is to be noted that the term "DOCSIS" in this document is understood to refer to DOCSIS version 1.1 or later, unless explicitly specified otherwise. Implementations of eCMs will refer to the corresponding DOCSIS versions and associated requirements in this document and DOCSIS specifications for compliance.

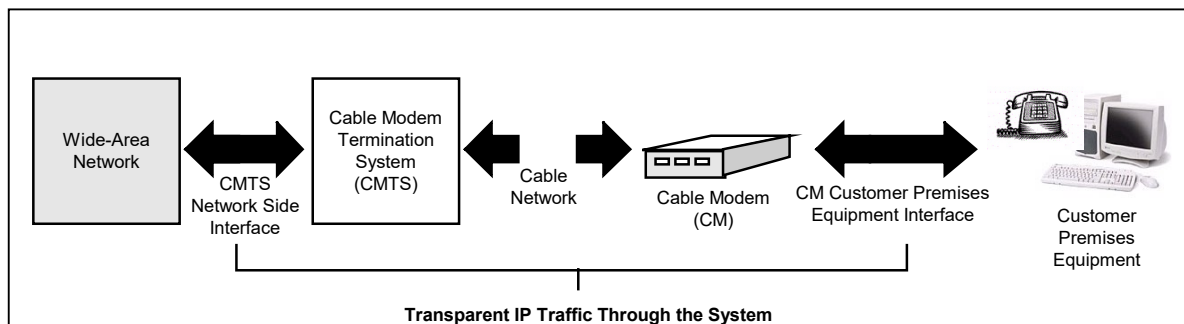


Figure 1. Transparent IP Traffic Through the Data-Over-Cable System

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

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 an IPcablecom 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), IPcablecom, and 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.
- To provision an E-MTA, both the DOCSIS and IPcablecom 1.5 provisioning steps **MUST** be performed. The eMTA **MUST** have its own IP address, different from the IP Address(es) of the eCM. The eMTA **MUST** also have its own MAC address, different from the MAC address of the eCM. Furthermore, the E-MTA **MUST** be able to operate in environments where the eMTA IP address may be in the same, or different subnet as the eCM.

- IPCablecom requires a unique FQDN for the MTA-component in the embedded-MTA. This FQDN MUST be included in the DHCP OFFER and DHCP ACK messages to the MTA-component. IPCablecom makes no additional FQDN requirements on the CM component in the embedded-MTA beyond those required by DOCSIS. Mapping of the FQDN to IP address MUST be configured in the network DNS server and be available to the rest of the network.
- IPCablecom 1.5 embedded-MTA provisioning MUST use DHCP Option-12 and Option-15 to deliver the MTA FQDN to the E-MTA.
- IPCablecom 1.5 embedded-MTA provisioning MUST support two separate configuration files, a DOCSIS-specified configuration file for the CM component, and an IPCablecom-specified configuration file for the MTA component.
- The embedded-MTA is outside the IPCablecom network trust boundary as defined in the IPCablecom architecture document [32].
- IPCablecom 1.5 E-MTA MUST support DOCSIS software download as defined in the corresponding eCM DOCSIS Specification. A single DOCSIS software download MUST be used to upgrade software for both the eCM and the eMTA.
- IPCablecom 1.5 MUST support use of SNMPv2c co-existence for network management operations for devices provisioned under the Basic Flow or the Hybrid Flow and SNMPv3/v2 co-existence for network management operations when the device is provisioned under the Secure Flow.
- IPCablecom 1.5 embedded-MTA provisioning minimizes the impact to DOCSIS devices (CM and CMTS) in the network.
- Standard server solutions (TFTP, SNMP, DNS, etc.) are preferable. It is understood that an application layer may be required on top of these protocols to coordinate IPCablecom 1.5 embedded-MTA provisioning.
- Where appropriate, the DOCSIS management protocols are supported (for example SNMP).

5.3 IPCablecom Reference Architecture

Figure 2 shows the reference architecture for the IPCablecom 1.5 network. Refer to the IPCablecom Architecture Document [32] for more detailed information on this reference architecture.

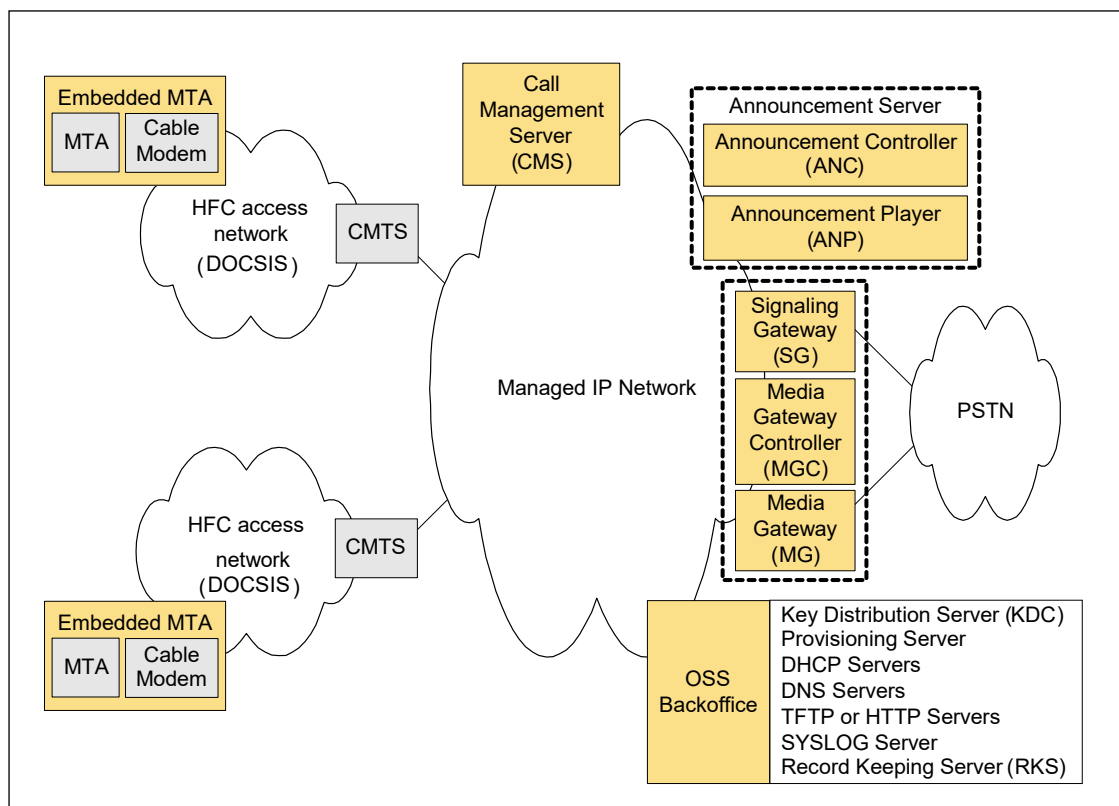


Figure 2. IPCablecom 1.5 Network Component Reference Model

5.4 Components and Interfaces

This figure represents the components and interfaces discussed in this document. All the IPCablecom specifications have a similar diagram indicating which interfaces of the IPCablecom Architecture are affected by a particular specification.

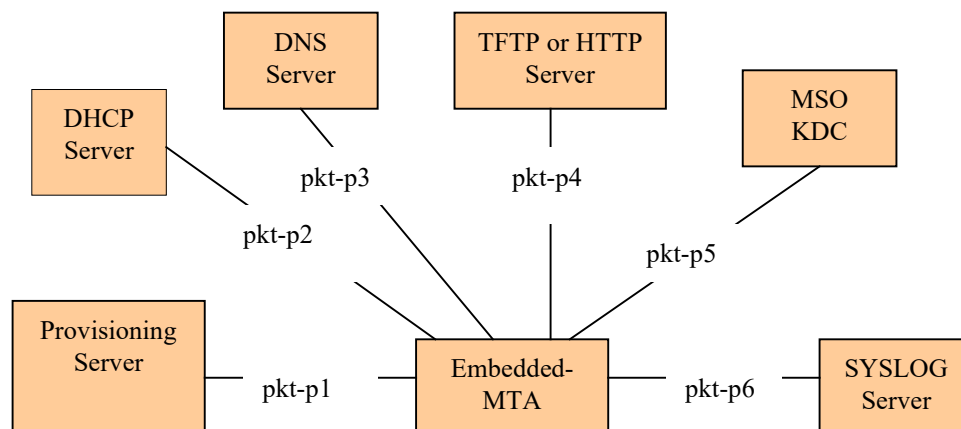


Figure 3. IPCablecom Provisioning Interfaces

5.4.1 MTA

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

5.4.1.1 MTA Security Requirements

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

- The MTA device MIB is structured to represent the assignment of MTA endpoints to a CMS. For more information on the security association between an MTA and a CMS refer to [5].
- 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 $\leq$ current time + PKINIT Grace Period, in which case the MTA MUST obtain a fresh ticket for the same CMS.)
- In the case that a CMS FQDN maps to multiple IP addresses, the MTA MUST initially establish a pair of IPsec Security Associations with one of the IP addresses returned by the DNS server. The MTA MAY also initially establish IPsec Security Associations with the additional CMS IP addresses. Please refer to [5] for more information.

If the MTA already has a pair of active Security Associations (inbound and outbound) with a particular CMS IP address, the MTA MUST NOT attempt to establish additional Security Associations with the same IP address.

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

5.4.1.2 MTA SNMP Requirements

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

- MTA SNMPv3 security is separate and distinct from 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.
- In Secure Flow, the MTA MUST support SNMPv3 and SNMPv2c based device management as defined in [8] and [52].

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

- SNMPv2c initialization MUST be completed immediately after the DHCP phase.
- SNMPv2c based device management as defined in [52].

The MTA MUST implement the Management Information Base (MIB) modules as described in [49] and specified in [2], [3], [13], [15], and [16]. If it also implements the IETF MIB modules as specified in [22], [23], and [24], the MTA MUST ensure that both sets of MIB modules can co-exist without any conflicting or ambiguous behavior.

MTAs implementing multiple MIB environments MUST support the DHCP option 'CL_V4_PACKETCABLE_MIB_ENV_OPTION' as specified in Section 7 and Section 8.8.

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

5.4.2 Provisioning Server

The Provisioning Server is made up of the following components:

- Provisioning Application - The Provisioning Application is responsible for coordinating the embedded-MTA provisioning process. This application has an associated SNMP Entity.
- Provisioning SNMP Entity - The provisioning SNMP entity MUST include a trap/inform handler for provisioning enrollment and the provisioning status traps/informs as well as a SNMP engine for retrieving device capabilities and setting the Configuration filename and access method. Refer to the IPCablecom MTA MIB ([2], [22]) for a description of the MIB accessible MTA attributes.
- The Provisioning Server MUST examine the "Device MIB Support" capability of the MTA (specified in Section 10.23) to choose the MIB modules that can be used to specify the MTA configuration file.

The interface between the Provisioning Application and the associated SNMP Entity is not specified in IPCablecom 1.5 and is left to vendor implementation. The interface between the Provisioning Server and the TFTP Server is not specified in IPCablecom 1.5 and is left to vendor implementation.

5.4.3 MTA to Telephony Syslog Server

The IPCablecom MTAs MUST implement Management Event Mechanism as per [14], which includes the support for Syslog server.

The IPCablecom MTAs MUST also implement all the IPCablecom Provisioning Management Events described in Appendix A of [14].

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 6, 7, 12, 15, 43, 60 and DHCP option code 122 (defined in [11]). Option code 12 (Host Name) and 15 (Domain Name) MUST form a Fully Qualified Domain Name and MUST be resolvable by the DNS server.

The DHCP server MUST accept and support broadcast and unicast messages per RFC 3396 [10] from the MTA DHCP client.

- The DHCP server MUST include the MTA's assigned FQDN in the DHCP OFFER and DHCP ACK messages to the MTA-component of the embedded-MTA. Refer to RFC 2131 [1] for details describing the DHCP OFFER message.

5.4.5 MTA to Provisioning Application

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

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

- The Provisioning Application MUST use only SNMPv3 to provision devices in the Secure Flow. The support of the Basic and Hybrid Flows is optional for the Provisioning Application. If the Basic and Hybrid Flows are supported, the Provisioning Application MUST use only SNMPv2c to provision devices in the Hybrid or Basic Flow.
- The Provisioning Application MUST provide SNMPv3 and SNMPv2c for device management.
- The Provisioning Application MUST support online incremental device/subscriber provisioning using SNMP.
- MTA MUST Specify all of its Capabilities in DHCP Option-60 in accordance with Section 10.
- 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 IPCablecom 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 unless provisioned to do so with information corresponding to the "pkteMtaDevCmsIpsecCtrl" MIB Object.

5.4.7 MTA to Security Server (KDC)

The interface between the MTA and the Key Distribution Center (KDC) MUST conform to the IPCablecom 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 delivered by DHCP Option 122 sub-option 5 (see Section 8.1.4).

AS-REQ/REP exchange backoff and retry mechanism of the Kerberized SNMPv3 key negotiation defined in [5] is controlled by the values delivered by DHCP Option 122 sub-option 4 (see Section 8.1.3) or by the default values of the corresponding MIB objects in the Realm Table if sub-option 4 is not present in the DHCP Option 122.

5.4.8 MTA and Configuration Data File Access

This 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 MTA MAY support HTTP access method for downloading the MTA configuration data file.

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

5.4.9 DOCSIS Extensions for MTA Provisioning

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

- eCMs that can obtain IP configuration information from multiple DHCP servers MUST use the primary DHCP server - designated to provide the eCM configuration information - for obtaining IPCablecom specific options (refer to [19] for more information).

- eCMs relying on DHCPv4 for IPCablecom specific information MUST implement DHCP option code 122 (as specified in [31]) and communicate the Telephony Service Provider's DHCPv4 Server information to the eMTA (as per Section 7 of this document).
- eCMs relying on DHCPv6 for IPCablecom specific information MUST implement the DHCP option code OPTION_VENDOR_OPTS(17) (as specified in [21]) and the "CableLabs Client Configuration" DHCPv6 option code CL_OPTION_CCC (as specified in [20]) to communicate the Telephony Service Provider's DHCPv4 Server information to the eMTA.

6 PROVISIONING OVERVIEW

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

6.1 Device Provisioning

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

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

When the device is provisioned using the "Secure Flow", the MTA device **MUST** be able to verify the authenticity of the configuration file it downloads from the server. The "Secure Flow" generated configuration file is "signed" and may be "sealed". Please refer to [5] for further information.

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

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

6.2 Endpoint Provisioning

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

The MTA **MUST** follow the requirements defined in the IPCablecom Security Specification [5] for NCS Kerberized Key Management, independently of the provisioning flow (Secure, Hybrid or Basic Flow) the MTA was provisioned with.

6.3 Secure Flow Provisioning State Transitions

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

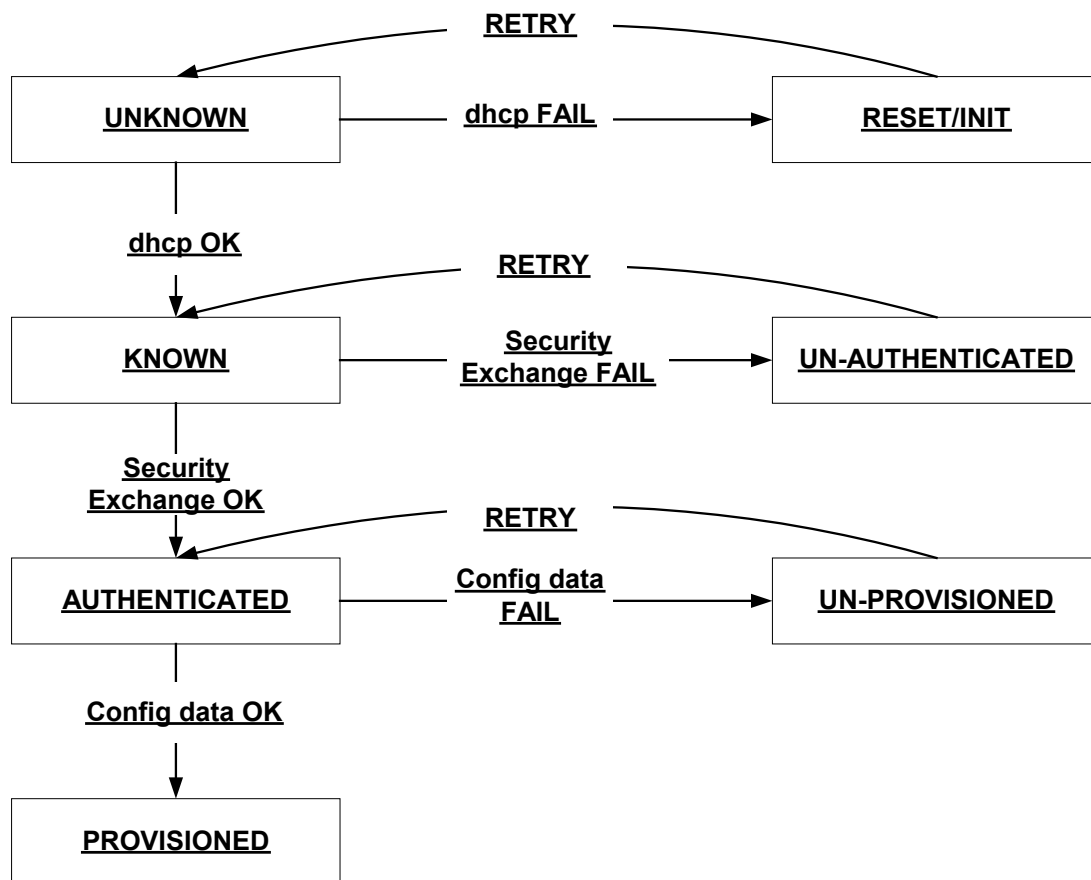


Figure 4. Device States and State Transitions for Secure Flow Provisioning