



**SOCIETY OF CABLE
TELECOMMUNICATIONS
ENGINEERS, INC.**

ENGINEERING COMMITTEE
Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 24-11 2009

IPCablecom 1.0 Part 11: Internet Signaling Transport Protocol (ISTP)

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) Standards are intended to serve the public interest by providing specifications, test methods and procedures that promote uniformity of product, interchangeability 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 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 members, whether used domestically or internationally.

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

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. SCTE 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 standard 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 web site at <http://www.scte.org>.

All Rights Reserved

© Society of Cable Telecommunications Engineers, Inc. 2009
140 Philips Road
Exton, PA 19341

Note: DOCSIS® is a registered trademark of Cable Television Laboratories, Inc., and is used in this document with permission.

Table of Contents

1 INTRODUCTION	1
1.1 Purpose	1
1.2 Scope	1
1.3 Document Overview	2
1.4 Requirements Syntax	2
2 REFERENCES	3
3 TERMS AND DEFINITIONS	4
4 ABBREVIATIONS AND ACRONYMS	8
5 OVERVIEW AND BACKGROUND MOTIVATION	15
5.1 Service Goals	15
5.2 IPCablecom Reference Architecture	16
5.3 Introduction to ISTP	17
5.4 Specification Goals	19
5.5 Specification Interfaces	19
6 ARCHITECTURE	21
6.1 IPCablecom to PSTN	21
6.2 Signaling Architecture Network Model	22
6.2.1 Network Reliability	23
6.2.2 Guaranteed Performance	24
6.2.3 Performance Model	25
6.3 Protocol Stack	25
7 FUNCTIONAL AREAS	27
7.1 Mapping Relationships	27
7.1.1 SS7 numbering	28
7.1.2 IPCablecom numbering	28
7.1.3 ISTP numbering	29
7.2 Message Distribution	29
7.3 Mapping	29
7.4 Relationships	30
7.5 Initialization	30
7.6 Recovery	31
7.7 Dynamic Provisioning	31
7.8 Administration	31
7.9 Security	32
7.10 Maintenance	32
7.11 Measurement	32
7.12 Alarms	32
7.13 Congestion	32
7.14 Management of lower layers	32
8 PROTOCOL	33
8.1 General Requirements	33
8.1.1 Communication with the Lower Layers	33
8.1.2 Encoding Rules	33
8.1.3 SS7 Load-Sharing and Sequencing	33
8.2 Procedures	34

8.2.1 Registration of Circuit Identifiers.....	34
8.2.2 Activation of Registered Circuits.....	35
8.2.3 Registration of Subsystem Transactions.....	36
8.2.4 Activation of Registered Subsystem Transactions.....	37
8.2.5 Message Transfer.....	38
8.3 Failure Detection and Handling.....	39
8.3.1 Heartbeat.....	39
8.3.2 Signaling Gateway Procedures.....	40
8.3.3 MGC and CMS Procedures.....	41
8.4 Message Format.....	42
8.4.1 Message Types.....	42
8.4.2 Message Nature.....	44
8.4.3 Parameters.....	44
8.5 Messages.....	50
8.5.1 Circuit Registration and Activation Messages.....	50
8.5.2 Subsystem Transaction Registration and Activation Messages.....	52
8.5.3 Message Transfer.....	54
8.5.4 Flow Control.....	55
APPENDIX A. SCTP AND TCP USAGE RECOMMENDATIONS.....	59
A.1 SCTP Usage Recommendations.....	59
A.2 TCP Usage Recommendations.....	59
APPENDIX B. ISTP MESSAGE FLOWS AND TIMER DEFINITIONS.....	61
B.1 Timers.....	61
B.2 MGC Requests ISUP/TUP Service Procedure.....	62
B.3 MGC Terminates ISUP/TUP Service Procedure.....	63
B.4 Residential CA Requests TCAP Service Procedure.....	64
B.5 Residential CA Terminates TCAP Service Procedure.....	65
B.6 A Typical Origination Communication.....	66
B.7 800 Number Service.....	67
B.8 MGC Failover Procedure.....	68
B.9 MGC Switchover Procedure.....	69

List of Figures

FIGURE 1. TRANSPARENT IP TRAFFIC THROUGH THE DATA-OVER-CABLE SYSTEM	15
FIGURE 2. IPCABLECOM REFERENCE ARCHITECTURE	17
FIGURE 3. PROTOCOL DISTRIBUTION IN IPCABLECOM ELEMENTS	18
FIGURE 4. ISTP IN DECOMPOSED IPCABLECOM GATEWAY	21
FIGURE 5. ARCHITECTURE MODEL OF A FULLY DISTRIBUTED IPCABLECOM GATEWAY EMPLOYING N+K REDUNDANCY	24
FIGURE 6. SS7 SIGNALING GATEWAY PROTOCOL STACK MODEL USING SCTP	26
FIGURE 7. MGC REQUESTS ISUP/TUP SERVICE.....	62
FIGURE 8. MGC TERMINATES ISUP/TUP SERVICE.....	63
FIGURE 9. MGC REQUESTS TCAP SERVICE.....	64
FIGURE 10. CA TERMINATES TCAP SERVICE	65
FIGURE 11. A TYPICAL ORIGINATION COMMUNICATION.....	66
FIGURE 12. 800 NUMBER SERVICE	67
FIGURE 13. MGC FAILOVER PROCEDURE	68
FIGURE 14. MGC SWITCHOVER PROCEDURE	69

List of Tables

TABLE 1. MESSAGE FORMAT	42
TABLE 2. MESSAGE TYPES	43
TABLE 3. MESSAGE NATURE	44
TABLE 4. PARAMETER NAME REFERENCES	45
TABLE 5. CIRCUITRANGE	46
TABLE 6. DESTINATIONTYPE.....	46
TABLE 7. INACCESSIBILITYREASON	46
TABLE 8. ISUPCLIENTRETURNVALUE	47
TABLE 9. ISUPTRANSFERFORMAT	47
TABLE 10. QUALITYOFSERVICE.....	48
TABLE 11. ROUTINGLABEL.....	48
TABLE 12. SCCPPARTYADDRESS	49
TABLE 13. SUBSYSTEM	49
TABLE 14. TCAPCLIENTRETURNVALUE	50
TABLE 15. TCAPTRANSFERFORMAT	50
TABLE 16. CIRCUIT REGISTRATION	51
TABLE 17. CIRCUIT DE-REGISTRATION REQUESTS.....	51
TABLE 18. CIRCUIT ACTIVATION REQUESTS	51
TABLE 19. FORCED CIRCUIT DEACTIVATION INDICATION.....	52
TABLE 20. SUBSYSTEM REGISTRATION REQUESTS.....	52
TABLE 21. SUBSYSTEM DE-REGISTRATION REQUESTS.....	53
TABLE 22. SUBSYSTEM ACTIVATION REQUESTS	53
TABLE 23. FORCED SUBSYSTEM DEACTIVATION INDICATION.....	54
TABLE 24. ISUP-MESSAGE-TRANSFER	54
TABLE 25. TCAP-MESSAGE-TRANSFER.....	55
TABLE 26. SIGNALING POINT INACCESSIBLE	56
TABLE 27. SIGNALING POINT ACCESSIBLE	56
TABLE 28. SUBSYSTEM INACCESSIBLE	57
TABLE 29. SUBSYSTEM ACCESSIBLE	57
TABLE 30. SIGNALING POINT CONGESTION.....	57
TABLE 31. LOCAL CONGESTION	58
TABLE 32. ISTP MESSAGE RESPONSE TIMERS	61

1 INTRODUCTION

1.1 Purpose

This specification describes the Internet Signaling Transport Protocol (ISTP) for IPCablecom PSTN Signaling Gateways. ISTP is being defined as part of the IPCablecom project. It is issued to support design and field-testing leading to the ability of multiple vendors to manufacture interoperable hardware and software.

ISTP is a protocol that provides a signaling interconnection service between the IPCablecom network control elements (Call Management Server and Media Gateway Controller) and the PSTN SS7 Signaling network through the SS7 Signaling Gateway. ISTP contains features for initialization; address mapping from the SS7 domain to the IP domain; message delivery for SS7 ISUP and TCAP; congestion management, fault management, maintenance operations; and redundant configuration support. ISTP bridges the gap between basic IP transport mechanisms and application level signaling. Although not a translation of the SS7 MTP3 and SCCP protocols, ISTP implements analogues to some of the MTP3 and SCCP functions in a fashion appropriate to distributed systems communicating over an IP network.

In order to meet the performance and reliability requirements mandated by the IPCablecom Service Requirements Specification and SS7 interconnection, ISTP requires the services of an underlying reliable transport service. The reliable transport provided by the Stream Control Transport Protocol (SCTP) as defined in the IETF SIGTRAN is the preferred solution; however, managed TCP over IP network may be used as an alternative.

In order to guarantee at least a base level of interoperability between SS7 Signaling Gateways and the IPCablecom control elements, an addendum to this specification is planned that will detail an IPCablecom usage profile for ANSI ISUP and TCAP. A provisionable option will allow the Signaling Gateways to pass the native SS7 signaling messages instead of the profiled ANSI messages.

1.2 Scope

This document addresses the protocol to implement SS7 signaling interconnection in a distributed IPCablecom PSTN Gateway architecture. Specifically, it defines the messages and procedures for transporting SS7 ISUP, TCAP, and TUP messages between the IPCablecom control functions (Media Gateway Controller and Call Management Server) and the SS7 Signaling Gateway.

Areas beyond the scope of the document include:

- Address layer management (SNMP), security, and measurements; these are covered in other IPCablecom documentation.
- Implementation and vendor dependant issues, such as performance, functional distribution, network configuration, etc.
- Details about CMS, MGC, and other media communication applications.

In addition, note that from time to time this document refers to the voice communications capabilities of an IPCablecom network in terms of "IP Telephony." 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 and are beyond the scope of this document. Nothing in this document 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 should be recalled 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, and that these differences may be significant for legal/regulatory purposes. Moreover, while reference is made here to "IP Telephony," it should be recognized that this term embraces a number of different technologies and network architecture, each with different potential associated legal/regulatory obligations. No particular legal/regulatory consequences are assumed or implied by the use of this term.

1.3 Document Overview

This document describes an IPCablecom protocol for interworking IP and SS7 networks to support voice-over-IP (VoIP) PSTN Gateways and Controllers, meeting commonly accepted quality, performance and reliability requirements. The IPCablecom protocol described in this document will be referred to as the IPCablecom Internet Signaling Transport Protocol (ISTP) protocol.

This document is structured in the following main sections:

- The overview provides a high level introduction to the protocol. In addition, it describes the motivation for developing ISTP and a summary of the underlying goals and assumptions for its design.
- The architecture section describes a model of the networks, elements, and nodes of the IP and SS7 networks, and the relationships between the elements of the networks.

The functional areas section describes the required capabilities in the areas of:

- Address and name mapping between the SS7 and IP networks, and relationships between important identifiers.
- Message distribution to network applications and nodes.
- ISTP level initialization, recovery, validation, monitoring, alarm management, congestion control, performance, security, and configuration.
- Management of lower layers, including session establishment and recovery without causing duplication of messages and other errors.
- The protocol description section presents the actual ISTP messages, including encoding of the parameters, which are based on binary formats. Associated with messages are the procedures that will be required for an ISTP implementation.
- The appendices contain a TCP and a SCTP implementation guide, example call flows, a list of IPCablecom interface specifications, and acknowledgements.

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.

2 REFERENCES

The following documents contain provisions, which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the documents listed below.

- [1] ANSI T1.111 Signaling System No. 7 (SS7) - Message Transfer Part (MTP), 1996, www.ANSI.org.
- [2] Data-Over-Cable Service Interface Specifications, Cable Modem to Customer Premise Equipment Interface Specification, CMCI, CM-SP-CMCI-C01-081104 , November 4, 2008, Cable Television Laboratories, Inc.
- [3] ANSI/SCTE 23-1 2005, DOCSIS 1.1 Part 1: Radio Frequency Interface
- [4] IETF RFC 791, Defense Advanced Research Projects Agency, Internet Protocol, September 1981.
- [5] IETF RFC 821, J. Postel, Simple Mail Transfer Protocol (SMTP), August 1982.
- [6] IETF RFC 2960, R. Stewart, Q. Xie, K. Morneault, et. al., Stream Control Transport Protocol (SCTP), December 2000.
- [7] ITU-T Recommendation Q.704, Specifications of Signaling System No. 7 - Message Transfer Part, July, 1996.
- [8] ITU-T Recommendation Q.706, Specifications of Signaling System No. 7 Message Transfer Part Signaling Performance, March 1993.
- [9] ITU-T Recommendation Q.706, Specifications of Signaling System No. 7 signaling performance in the Telephone Application, March 1993.
- [10] ITU-T Recommendation Q.709, Specifications of Signaling System No. 7-Hypothetical Signaling Reference Connection, March 1993.
- [11] ITU-T Recommendation Q.714, Specifications of Signaling System No. 7 - Signaling Connection Control Part, July, 1996.
- [12] ITU-T Recommendation Q.761, Functional Description of the IDSN User Part of Signaling System No. 7, (September, 1997).
- [13] ITU-T Recommendation Q.762, General Function of messages and Signals of the IDSN User part of System No. 7 (September, 1997).
- [14] LSSGR: Switch Processing Time Generic Requirements Section 5.6, June 1995.
- [15] ANSI/SCTE 24-1, 2009, IPCablecom 1.0 Part 1: Architecture Framework for the Delivery of Time-Critical Services Over Cable Television Networks Using Cable Modems.
- [16] ANSI/SCTE 24-3 2009, IPCablecom 1.0 Part 3: Network Call Signaling Protocol for the Delivery of Time-Critical Services over Cable Television Using Data Modems.
- [17] ANSI/SCTE 24-12 2009, IPCablecom 1.0 Part 12: Trunking Gateway Control Protocol (TGCP).
- [18] Telcordia Technologies Generic Requirements GR-1364-CORE, Issue 1.
- [19] Telcordia Technologies TR-TSY-000511, LSSGR: Service Standards, Section 11, Issue 2, July 1987.

3 TERMS AND DEFINITIONS

The following is a master list of terms and definitions used in IPCablecom 1.0:

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 the 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 any one 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 head-end toward the subscriber location.

Encipherment	A method used to translate information in plaintext into ciphertext.
Encryption	A method used to translate information in plaintext into ciphertext.
Encryption Key	The key used in a cryptographic algorithm to translate the plaintext to ciphertext.
Endpoint	A Terminal, Gateway or MCU.
Errored Second	Any 1-sec interval containing at least one bit error.
Event Message	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 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 ISO Layer 3 and Layer 4 header information. This information includes source/destination IP addresses, source/destination port numbers, protocol ID. Multiple multimedia streams may be carried in a single IP Flow.
Gateway	Devices bridging between the IPCablecom 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 IPCablecom network.
H.323	An ISO standard for transmitting and controlling audio and video information. The H.323 standard requires the use of the H.225/H.245 protocol for communication control between a “gateway” audio/video endpoint and a “gatekeeper” function.
Header	Protocol control information located at the beginning of a protocol data unit.
Integrity	A way to ensure that information is not modified except by those who are authorized to do so.
IntraLATA	Within a Local and 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.
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 IPCablecom 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 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 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 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 head-end.
X.509 certificate	A public key certificate specification developed as part of the ITU-T X.500 standards directory.

4 ABBREVIATIONS AND ACRONYMS

The following is a master list of abbreviations and acronyms used in IPCablecom 1.0:

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 head-end which implements the DOCSIS RFI MAC protocol and connects to CMs over an HFC network.

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. See Appendix C.
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
F-link	F-Links are SS7 links that directly connect two SS7 end points, such as two SSPs. 'F' stands for "Fully Associated".
FQDN	Fully Qualified Domain Name. Refer to IETF RFC 821 for details.
GTT	Global Title Translation
HFC	Hybrid Fiber/Coax(ial [cable]). 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.
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 X509 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 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 information on customers 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.
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 IP/Cablecom 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, 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 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.

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 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 IPCablecom.
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 that is used to provide the services of authentication and encryption. 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 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 that is 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 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 OVERVIEW AND BACKGROUND MOTIVATION

5.1 Service Goals

Cable operators are interested in deploying high-speed data and multimedia communications services on cable television systems. Various cable operators, have prepared a series of interface specifications that permit the early definition, design, development, and deployment of packetized data-based services over cable systems on an uniform, consistent, open, non-proprietary, multi-vendor interoperable basis. The intended system enables Internet Protocol (IP) based voice communications, video, and data services to be provided to the customer over an all-coaxial or hybrid-fiber/coax (HFC) cable access network by utilizing the data over cable service interface specification (DOCSIS) standard as the basic foundation for data transport. This is shown in simplified form in Figure 1.

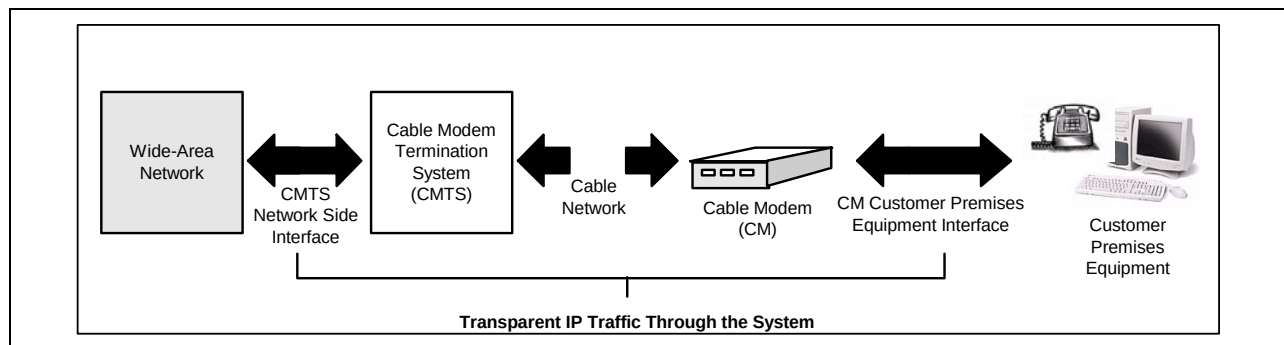


Figure 1. Transparent IP Traffic Through the Data-Over-Cable System

The transmission path over the cable system is realized at the headend by a cable modem termination system (CMTS) and at each customer location by a cable modem (CM). At the headend (or hub), the interface to the data-over-cable system is called the cable modem termination system-network-side interface (CMTS-NSI). At customer locations, the interface is called the cable-modem-to-customer-premises-equipment interface (CMCI). The intent is for operators to transfer IP traffic transparently between these interfaces, thereby providing the basic transport mechanism for databased multimedia services.

When providing voice and other multimedia services over the DOCSIS access network; many issues need to be addressed for incoming and outgoing communications. These issues include but are not limited to:

- Voice or other media content conversion.
- Call control signaling.
- Quality of service control.
- Call control signaling interoperability with the existing public network.
- Media interfaces to the existing public network.
- Data transactions to public databases.
- Routing mechanisms.
- Billing.
- Operations and maintenance.
- Security.
- Privacy.

The IPCablecom project is addressing these issues through the development and publication of reference architecture and a series of corresponding interface specifications. This specification, the IPCablecom Internet Signaling Transport Protocol (ISTP) addresses the issue of call control signaling interoperability with the existing public network.

5.2 IPCablecom Reference Architecture

The conceptual diagram in Figure 2 portrays a high level architectural view of the IPCablecom network.

Subscriber equipment consists of a Media Terminal Adapter (MTA), the primary purpose of which is to provide a gateway between the subscriber-side voice/video media devices and the rest of the IPCablecom network. Two types of MTAs exist. The first is a standalone MTA which connects via a local area network (LAN) interface (e.g., IEEE 802.3) to a DOCSIS cable modem. The second is an embedded MTA, which integrates the standalone MTA functions with the DOCSIS cable modem (CM) media access control (MAC) and physical layer (PHY) functions in the same physical package.

Physical connectivity to the backbone consists of an all-coax or a hybrid fiber-coax (HFC) DOCSIS enabled cable access network with DOCSIS 1.1 quality-of-service (QoS). The DOCSIS HFC access network terminates at the head end Cable Modem Termination System (CMTS). The CMTS provides either a bridging point or a routing point to the backbone managed IP network.

The call management server (CMS) provides control, routing, and signaling services in connection with voice communications provided via IPCablecom. It is responsible for authorization and plays a roll in feature implementation. The media servers provide support services for media streams such as conference mixing bridges and announcement servers.

CMS is a meta-term for a collection of functions (both specified and unspecified within IPCablecom) within a server or cluster of servers that work together to perform "line-side" control functions within an IPCablecom network. The simplest way to think of a CMS is to imagine the functions of a class 5 switch call controller being extrapolated and placed into a server farm. The CMS includes a minimum of a call agent and a gate controller. It may have feature and routing logic. It may or may not contain a media gateway controller, meaning that it can implement some class 4 functionality as well as class 5. A sip-proxy may also be contained within a CMS, although IPCablecom 1.0 doesn't include sip in the architecture.

A Call Agent is a specific control function contained within the CMS. It implements the server side of the protocol interface and controls MTAs. The MGC is a specific control function that may be contained within a CMS or may be standalone in the network. It implements the server side of the TGCP protocol interface and is used to control PSTN media trunking gateways.

The public switched telephone network (PSTN) gateway provides access from the subscriber network into the PSTN network. For outgoing communications, the media gateway (MG) converts the voice samples arriving in RTP packets into the appropriate TDM format and delivers the resulting voice stream to the public network. The media gateway controller (MGC) provides signaling information related to the communication to the PSTN through the services of the signaling gateway (SG). This signaling information exchanged with the PSTN is used by the components of the IPCablecom network to manage the communication's progress and provide required features and functionality. In addition, IPCablecom gateways also interwork with the public databases of the PSTN using SS7 TCAP queries, allowing the IPCablecom network to query for publicly available data (800 numbers, local number portability service, credit card data, etc.).

For incoming communications, IPCablecom equipment will convert arriving TDM circuit voice to RTP packets carrying appropriately coded samples. It will also take the incoming communication related SS7 ISUP signaling and convert it to signaling understood by IPCablecom devices.

The OSS back office provides support services such as billing, provisioning, fault determination, problem resolution, and other support services.

Note that ISTP makes no assumptions on how the CMS and MGC and other ISTP-User functions are distributed or physically located: they all MAY be collocated, each distributed on separate computers, or all distributed as separate

nodes and processes across a wide network and a large number of computers. ISTP was designed to handle all these cases.

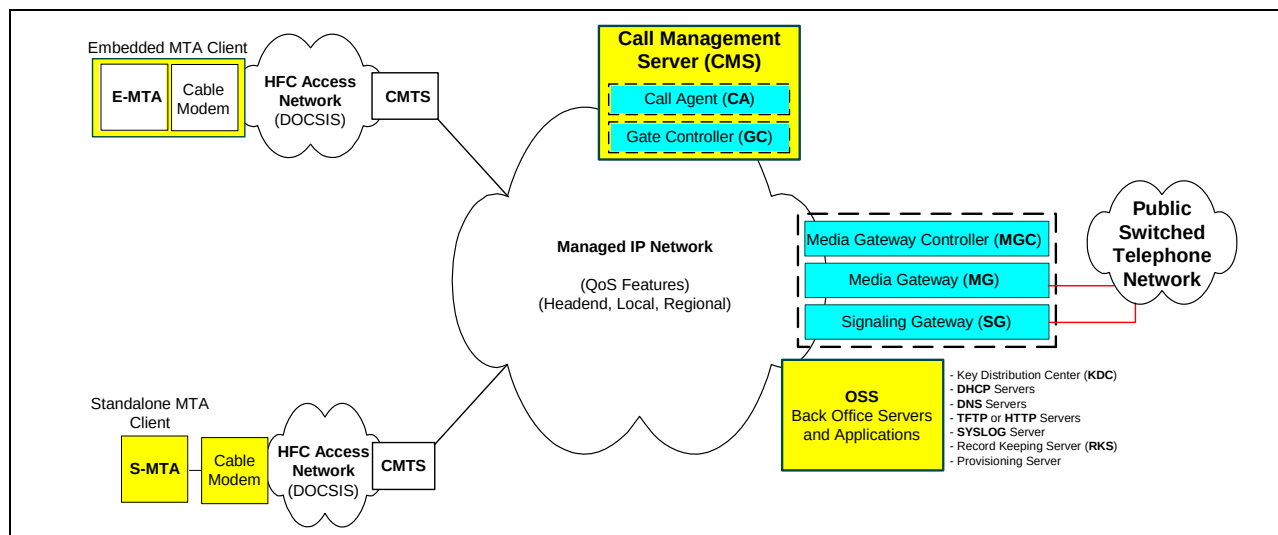


Figure 2. IPCablecom Reference Architecture

5.3 Introduction to ISTP

ISTP contains features for initialization; address mapping from the SS7 domain to the IP domain; message delivery for SS7 Integrated Services Digital Networks (ISDN) User Part (ISUP), Transaction Capabilities Application Protocol (TCAP), and Telephony User Part (TUP) messages; congestion management; fault management; maintenance operations; and redundant configuration support. ISTP bridges the gap between basic IP transport mechanisms and application level signaling. Although not a translation of the SS7 Message Transport Protocol 3 (MTP3) and Signaling Connection and Control Protocol (SCCP) protocols, ISTP implements analogues to some of the MTP3 and SCCP functions in a fashion appropriate to distributed systems communicating over an IP network.

Thus ISTP "remotes" transparently the ISUP and TCAP functions into distributed elements and keeps the operational sensitive and computational intensive SCCP/MTP2/MTP2 SS7 stack elements in the Signaling Gateway (see Figure 3). This breakdown also allows ISTP-User applications to have access to all the (raw) TCAP and ISUP data, which may be necessary for some advanced features. It provides the maximum isolation from SS7 details while providing full transaction and signaling information. It also allows new ISTP-user applications that require other SS7 application part protocols, such as GSM MAP and IS41 MAP, to be added in a graceful and backward compatible manner by installing the MAP agents over ISTP as needed.