SCTE | STANDARDS

Data Standards Subcommittee

AMERICAN NATIONAL STANDARD

ANSI/SCTE 24-11 2016 (R2022)

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

NOTICE

The Society of Cable Telecommunications Engineers (SCTE) 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, interoperability, interchangeability, best practices, and 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.

SCTE 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.

NOTE: The user's attention is called to the possibility that compliance with this document may require the use of an invention covered by patent rights. By publication of this document, no position is taken with respect to the validity of any such claim(s) or of any patent rights in connection therewith. If a patent holder has filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, then details may be obtained from the standards developer. 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 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 web site at https://scte.org.

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.

Document Types and Tags

Document Type: Specification
Document Tags:

☐ Test or Measurement	☐ Checklist	☐ Facility
☒ Architecture or Framework	☐ Metric	☒ Access Network
☐ Procedure, Process or Method	☐ Cloud	☐ Customer Premises

Document Release History

Release	Date
SCTE 24-11 2000	*3/28/2001*
SCTE 24-11 2006	*5/19/2006*
SCTE 24-11 2009	*6/5/2009*
SCTE 24-11 2016	*10/7/2016*

Note: This document is a reaffirmation of SCTE 24-11 2016. No substantive changes have been made to this document. Information components may have been updated such as the title page, NOTICE text, headers, and footers.

Table of Contents

List of Figures

List of Tables

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 dependent 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 Requirements and Conventions

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 event useful, but the full implications should be understood and the case carefully weighted 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.

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.

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.

[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 Premises Equipment Interface (CMCI) Specification, CM-SP-CMCI-C01-081104, http://www.cablelabs.com/specification/cable-modem-to-customer-premise-equipment-interface-specification/, Cable Television Laboratories, Inc.

[3] ANSI/SCTE 23-01 2010, 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 24-01 2016, IPCablecom 1.0 Part 1: Architecture Framework for the Delivery of Time-Critical Services over Cable Television Networks Using Cable Modems.

[16] ANSI/SCTE 24-03 2016, 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, 2016, 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 Bode. An option in block ciphers that combines (XORs) 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 IPCablecom 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-Ream 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 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.

5.2 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.

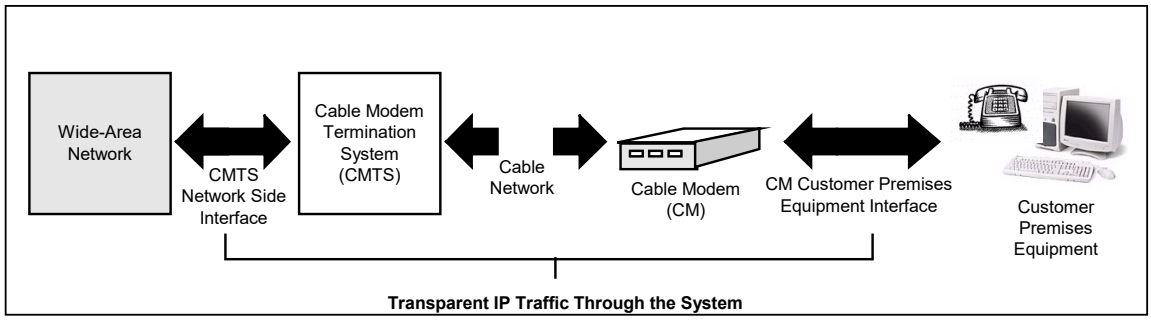

Figure 1. Transparent IP Traffic Through the Data-Over-Cable System

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.

5.3 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.

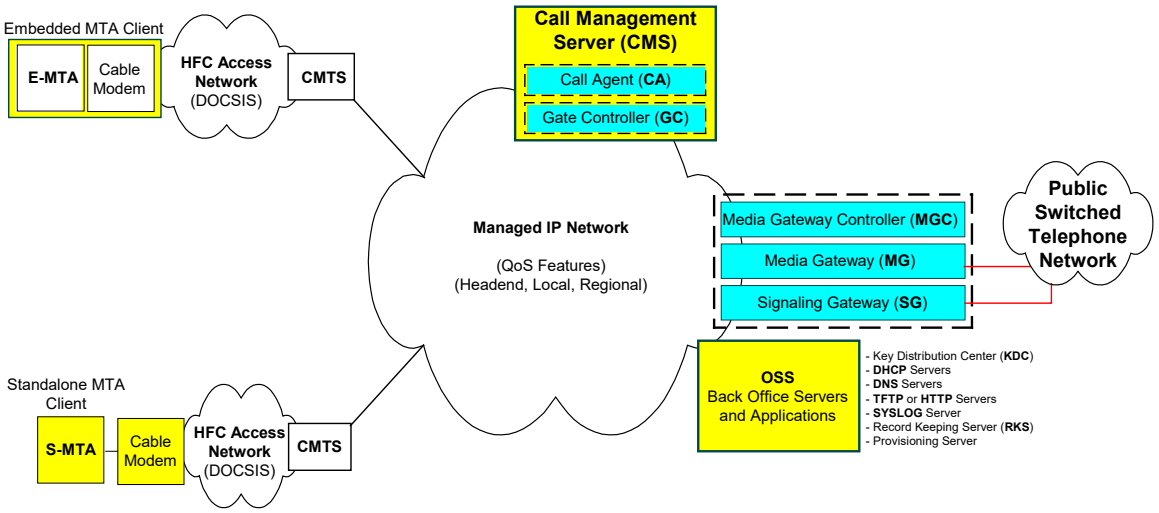

Figure 2. IPCablecom Reference Architecture

5.4 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.

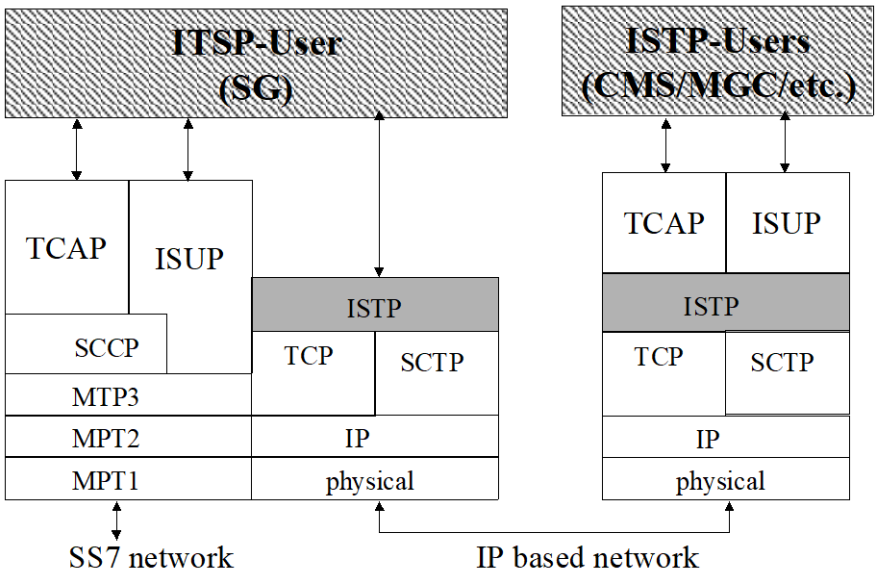

Figure 3. Protocol Distribution in IPCablecom Elements

The ISTP is designed to support a wide variety of configurations, ranging from a non-redundant SS7 Signaling Gateway serving a single non-redundant Media Gateway Controller to a distributed, fully redundant SS7 Signaling Gateway serving multiple distributed and redundant Media Gateway Controllers and Call Management Servers, and potentially other network elements.

Note: the term ISTP-User will be a generic term for any element, node, or process that uses the ISTP stack for signaling communications. For the first phase of IPCablecom this include the CMS, MGC, and SG. In the future, other types of elements may include the stack.

The ISTP contains functions for:

- Initialization.
- Registration of Circuit IDs with the SS7 Gateway
- Address Mapping Between the SS7 and IP domains
- ISUP Maps Based on Point Code and Circuit Identification Code
- TCAP Maps Based on Point Code and Transaction ID
- ISUP/TCAP Message Delivery Using Reliable Transport
- Maintenance Operations

- Activation/De-activation of Circuit IDs within the SS7 Gateway (The actual physical circuits terminate on the Media Gateway)
- Error Recovery Due To Faults
- SS7 Signaling Point Inaccessible
- SS7 Signaling Network Inaccessible
- MGC Inaccessible
- CMS Inaccessible
- Error Recovery Due To Congestion
- Signaling Point Congested
- Signaling Link Congested
- MGC Congested
- CMS Congested

The above functions are implemented messages and procedures defined in section 8 of this document.

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 preferred is Stream Control Transport Protocol (SCTP) [6] as defined in the IETF SIGTRAN working group in RFC 2960 [6]. TCP can provide a workable solution, as long as the network is engineered properly, but SCTP is preferred. UDP is not considered an acceptable option, as it does not supply sufficient reliability to meet IPCablecom requirements.

In order to guarantee at least a base level of interoperability between SS7 Signaling Gateways and the IPCablecom call control elements, a normative (meaning that support is mandatory) 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.

5.5 Specification Goals

The goal of this specification document is to meet and satisfy the business and technical requirements of the cable industry and the IPCablecom project, including the following:

- Support for cable companies' penetration into residential and business markets for multi-media services, including voice.
- A low cost replacement for PSTN switching, peripheral, and control elements using IP based technology.
- A network that can provide higher level features (such as multi-media) in addition to the PSTN features.
- A transparent interface to the existing PSTN.
- An open architecture, that will support the interworking of multiple vendors' equipment in the same IPCablecom network.
- A scalable gateway architecture, allowing solutions ranging, for example, from the equivalent of a single T1 media gateway up to a system that is the equivalent of a large tandem switch supporting multiple central offices (about 40,000 trunks).
- An architecture that can achieve the same high degree of reliability and performance as the PSTN, while allowing for a "descoped" network (simplex connections) to support lower cost enterprise and customer premise implementations.

5.6 Specification Interfaces

The basic reference architecture (see Figure 2) involves two interface categories between the SS7 Signaling Gateway and the IPCablecom call control elements:

- *SS7 Signaling Gateway to Media Gateway Controller* – Enables signaling interconnection between the SS7 network and the Media Gateway Controller for SS7 ISUP message interworking. ISUP is used for out-of-band call signaling in the PSTN.
- *SS7 Signaling Gateway To TCAP User* – Enables signaling interconnection between the SS7 network and certain trusted entities ("TCAP Users") within the IPCablecom network, such as Call Management Servers and Media Gateway Controllers, for SS7 TCAP message interworking. TCAP is used primarily to query external PSTN databases for applications such as 800/888 calling and local number portability (LNP) routing.

For the first phase of IPCablecom, only ANSI versions of SS7 will be supported. However, ISTP can also support other versions including ITU and local country variants. In addition, the signaling gateway is required to handle a single point code only; but vendor implementations may choose to handle multiple point codes in one signaling gateway.

6 ARCHITECTURE

6.1 IPCablecom to PSTN

The ISTP is specified within the context of an architecture intended to interwork an IP-based cable network with the public switched telephone network (PSTN); this architecture is described in [15]. ISTP is specified with an initial focus on SS7 interworking with the PSTN only, but other legacy protocols, such as ISDN could be supported in the future. At this time, only the Call Management Server, the Media Gateway controller, and the Signaling Gateway use ISTP; however, the protocol is designed to support future network elements where access to the SS7 network or transactions from the SS7 network are needed.

There are three types of networks involved (see Figure 4):

- The first is the IP based packet network for transport of IP side signaling, voice, and data; this network can also be logically or physically partitioned to optimize performance and reliability for the various transported media, and there can be separate networks for the voice over IP and the signaling over IP packets.
- The second is the switched circuit network for transport of voice, fax, and modem data.
- The third is the SS7 signaling based network for reliable transport of critical signaling information. The SS7 signaling network signaling is used to control the switched circuit network. The SS7 signaling and switched circuit network together constitutes the PSTN.

The Call Management Server and Media Gateway Controller handle control information from end users or subscribers. To manage the network trunks and obtain public data in the PSTN, SS7 signaling information is exchanged with the PSTN via the signaling gateway. In this way, IP based elements can use SS7 messaging to manage and access the resources of the PSTN. Encoded voice IP packets are converted at the Media gateway and sent over dedicated PCM trunks. The Signaling Gateway is thus independent of the underlying voice communications activities of the IPCablecom network. Instead, it is only concerned with supporting interconnection between the cable IP packet network and the SS7 signaling network.

As the network migrates in the future to other networks beyond the switched circuit network, such as IP or ATM networks, ISUP and TCAP signaling will still be required to ensure cross network interoperability; this will be true whether the SS7 signaling runs over SCCP/MTP3/2/1 or over ATM or other protocol. In such a case the Signaling Gateway can modify its lower layers without impacting the ISTP-Users.

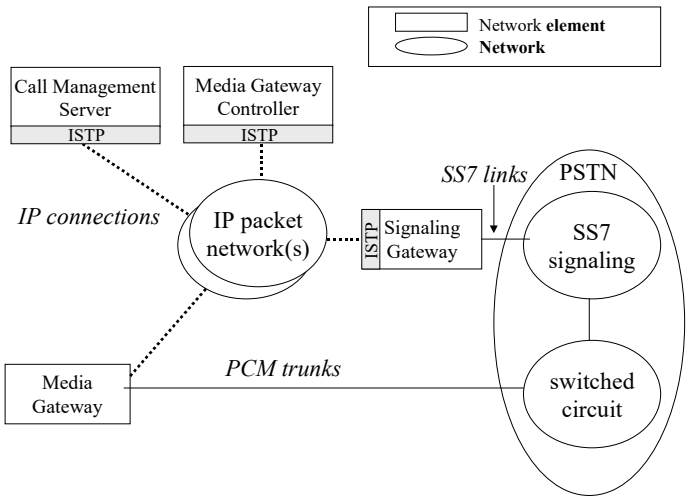

Figure 4. ISTP in Decomposed IPCablecom Gateway

6.2 Signaling Architecture Network Model

The ISTP focuses on supporting signaling interworking between the elements controlling the IP connections and the elements connected to the PSTN and SS7 networks. Given the requirements for performance, scalability, and reliability, a highly distributed and redundant network is assumed. ISTP supports both manual and autonomous recovery from failure in this network. A fully redundant network supporting these requirements is assumed to be "n+k" redundant; that is, there are n+k instances of any element, where n is the minimum number of elements required to handle traffic, and k is the number of spare elements that can take over for a failed element. The numbers, n and k, are set by traffic modeling, mean time to failure, repair analysis, and field experience to ensure that the total system availability is maintained if one or more elements fails. While ISTP was designed to a n+k model, it is useful to note that an active-standby (1+1) network, and a simplex (1+0) network are supported subsets of the n+k network model.

The signaling architecture for ISTP currently consists of three elements: Media Gateway Controllers, Call Management Servers, and Signaling Gateways (see Figure 2)[1]. Each element can contain one or more separate nodes (typically computers), with independent points of failure and IP network addresses that cooperate to provide a single function.

- A Signaling Gateway (SG) element is a collection of one or more Signaling Gateway Nodes (SGN). The function of the Signaling Gateway element is to allow for the interworking of the IP based IPCablecom network with the existing PSTN using SS7 signaling. It provides for the transport of higher level (TCAP, ISUP and, possibly in the future, TUP) SS7 signaling messages over IP, terminating the SS7 SCCP and MTP 3/2/1 layers at the SS7 network interface. The main goal of the SG is to isolate the various ISTP-Users from the details of the lower level SS7 protocols. The ISTP-Users only have to deal with the ISUP and TCAP parameters, which they have to know in any case to implement the advanced features required by subscribers. Only the SG has to handle the complex and operational sensitive SCCP, MTP3/2/1 layers.
- Each SG element has at least one unique SS7 point code (some vendor implementations MAY support multiple point codes), with multiple SS7 links. Each SG Node has one or more unique IP addresses within the IP network. For the remainder of this document the terms "Signaling Gateway" or "SG" shall be inferred to mean a "Signaling Gateway Element". Signaling Gateway nodes will be referred to as such using the acronym "SGN". A signaling gateway is required to handle a single point code only; however, particular vendor implementations can support multiple point codes on a single SG.
- A Media Gateway Controller (MGC) element is a collection of one or more Media Gateway Controller Nodes (MGCN). The function of the Media Gateway Controller element is to process the trunk side of an IPCablecom communication. The MGC is identified by a unique name (string). Each MGCN has one or more unique IP addresses within the IP network. For the remainder of this document, the terms "Media Gateway Controller" or "MGC" shall be inferred to mean "Media Gateway Controller element". Media Gateway Controller Nodes will be referred to as such or using the acronym "MGCN".
- A Call Management Server (CMS) element is a collection of one or more Call Management Server Nodes (CMSN). The function of the Call Management Server element is to perform Call Agent functions or SIP proxy functions for the subscriber side of an IPCablecom communication, including managing the needed media resources. It requires TCAP queries to implement local number portability (LNP), 800, and other services. Each CMSN has one or more unique IP addresses within the IP network. For the remainder of this document, the terms "Call Management Server" or "CMS" shall be inferred to mean "Call Management Server element". Call Management Server Nodes will be referred to as such or using the acronym "CMSN".

A Signaling Gateway appears as a single point code to the SS7 network, where it is viewed as a "signaling endpoint". The SG will manage the transfer of the appropriate messages to the correct ISTP-User element based on

[1] Note that the concept of an "element" is different from that of a "function", as used in the PSTN Gateway Architecture and Functional Requirements specification. In the above mentioned document, the term "function" was used to describe component parts of a logical partitioning of duties within a distributed IPCablecom PSTN gateway. The specification allows the logical component parts ("functions") to be combined or further decomposed for physical implementations. In this document, the term "element" refers to a physical instantiation of an IPCablecom function. Since the ISTP is only required when certain IPCablecom functions are implemented in separate physical instantiations ("elements"), this is the only case considered in this document.

the fixed trunk identity; with ISTP, the CID dynamically determines which elements (CMS/MGC/ANS) to use when routing a call.

It is thus possible for the ISTP to support multiple call models in different MGCs on the same network at the same time, or different vendors MGCs on the same network at the same time, or different versions of the same MGCs on the same network at the same time. For example:

- It can support a MGC that handles a set of BPX "enterprise" features and one that handles a set of central office "home subscriber" features.
- Based on the target trunk group identity, an incoming call can be routed to a "home subscriber" MGC from vendor A, or a "home subscriber" MGC from vendor B, depending on who owns the trunk.
- It is possible to load a "test release" of a beta of version 2 of a MGC, while the rest of the network is running version 1; only a limited subset of the calls will go to version 2 for testing, until the software release is proven, and the rest of the network can be upgraded.

These capabilities provide three high level benefits:

- It allows "second sourcing" of the MGC and other network elements on the same network
- It allows several operators to share a single SG, while each still retains ownership of the call by using CMS, MGC, ANS and billing elements.
- It supports piecewise software replacement and testing, and thus avoids having to upgrade all the MGCs at once, which may expose the total network to a software replacement failure.

6.2.1 Network Reliability

The architecture model was selected to support a network availability of the PSTN or higher (0.9999+) in a highly scalable fashion to allow for growth. Meeting this availability objective of will require service providers to implement several types of reliability and redundancy mechanisms in the network, such as:

- Redundant managed IP networks, with independent IP transport (WAN/LAN) and guaranteed delay and delivery times.
- Redundant independent network routers/local routers.
- Redundant connection, switching, and transport hardware.
- n+k element node redundancy.
- No-single point of failure, including geographical power (geographical distribution).

ISTP has been designed to support all of these options. Of course, the model allows non-redundant implementations as well (although a non-redundant network is not likely to meet the availability objective).

ISTP supports typical engineering guidelines, which require that stable communications to be recovered in the event of a single component failure. This allows subscribers in a "talking" state to continue talking in the event of a single node failure. No mechanisms are engineered into ISTP to guarantee the recovery of connections, which are in the process of being setup at the time of a component failure. Such mechanisms would have to be implemented at the application-signaling layer.

Figure 5 shows a fully distributed and redundant IPCablecom gateway, including the Media Gateway components. In the figure, ISTP would be used for signaling communication between the MGCNs and SGNs and between the CMSNs and the SGNs. While at first glance the ISTP network model appears complex, it should be noted that it is required to support an equivalent degree of signaling performance and reliability to the SS7 network, which has an even more complex network model. Also, where these requirements can be relaxed in implementation, the model resolves to a simpler subset that is supported by ISTP.

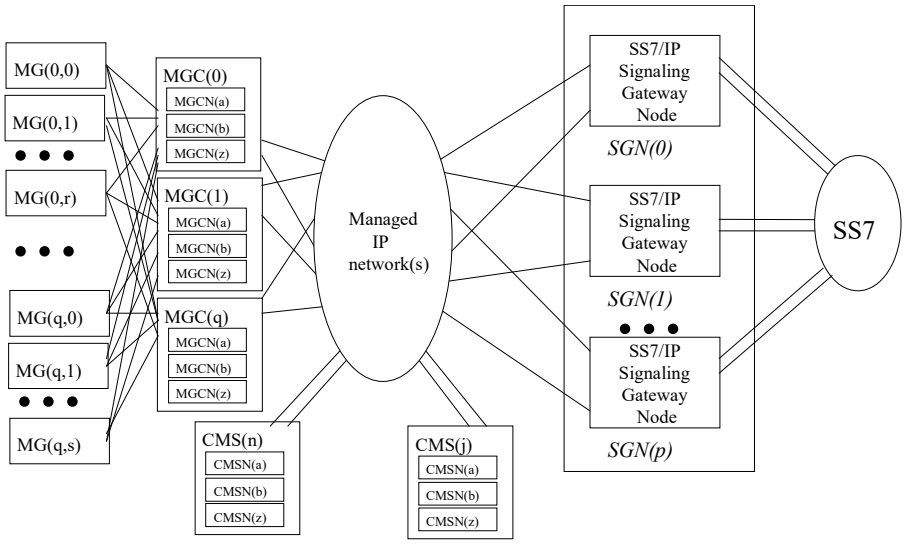

Figure 5. Architecture Model of a Fully Distributed IPCablecom Gateway Employing n+k Redundancy

6.2.2 Guaranteed Performance

An IPCablecom connection has the same performance requirements as a PSTN call. While the issue of performance is complex in a pure SS7 network, the mixture of IP and SS7, and the vendor dependent breakdown of performance budget makes performance a difficult area to define precisely.

ITU references are needed to handle budgets for international communications. Some performance references are found in [10], [18], [14], [8], [9], and [19].

Ignoring for the moment the differences between mean time and 95% time, and making simple assumptions about cross-office delay, a simple conclusion is that the performances of the total network should:

- Meet user expectations of one to two seconds for set up on national communications.
- Meet user exceptions of 2.5 - 5 seconds on international communications.

In order to meet these user expectations for communication set up, which consists of many messages and processes, each with their own delay budget, in many elements (as many as five) across the network, a single node needs to:

- Process critical SS7 ISUP events in under 50 ms.
- Process TCAP messages in less than 75 ms.

This expectation for real-time transport of signaling messages across the networks of less than 50 ms. delay mandates the following:

- A sub-layer protocol that:
  - is reliable
  - is real-time (less <25 ms for ISUP and 75 ms. for TCAP)
  - avoids duplicated and lost packets.
- Periodic "heartbeat" messages are sent point to point between each of the components so that each side continuously knows the availability status of the far end.
- Signaling messages can not be delayed by other IP traffic; this requires either a dedicated IP network (e.g., nailed up DS-0 links) for signaling or equivalent QoS provisioning to guarantee timely delivery.

6.2.3 Performance Model

The system should be scalable up to a reasonable size (one that does not compromise the reliability of the network).

A useful model for scalability validation assumes that the minimum sized Signaling gateway has a minimum of two links. SS7 links are dimensioned in pairs, so the size of a trunking network covered by a SG is in multiple of paired SS7 links, which themselves are only assumed to be 40% occupied each at maximum traffic (in case of a failure, the other link takes over all traffic at 80% occupancy).

One calculation that can be used as an example for a single pair SG is:

- That we assume a performance of 0.9 erlang for a ~13,000 trunks with ISUP call control and TCAP for LNP queries (800 / and credit card transactions not included).
- This will generate ~400 ISUP + TCAP messages/second. This will generate 5300 octets/s of ISUP + TCAP in each direction.
- This will fully occupy One pair of 56K signaling links (2 links).

At 0.2 erlang subscriber usage, this would cover 65,000 subscribers. It should be noted that this is not a hard limit, but merely a reasonable number of subscribers to place on one signaling gateway with the requisite minimum of two links in the PSTN network. With more links the system is scalable to higher numbers. On the IP side similar conditions hold, except that there is no requirement for separate signaling channels with 40% occupancy. However, the same rule is very good engineering practice, and the IP network should be designed with sufficient IP bandwidth redundancy to guarantee signaling in the event of a link failure.

6.3 Protocol Stack

The ISTP layer is designed to provide signaling interconnection for ISUP and TCAP messages over various forms of IP based systems.

Initially ANSI SS7 interfaces will be supported, but in the future other standards (such as ITU) and variants (such a TUP and country variants of ISUP and TCAP) to standards can be integrated into the protocol while retaining the backward compatibility of the ISTP stack. Also, other higher levels SS7 elements, such as TUP, GSM MAP, IS 41, etc. can be added in the future.

Initially, TCAP transactions are expected only to be generated from the IPCablecom network and sent to the PSTN; however support for unidirectional (call gapping) and TCAP transactions terminated on IPCablecom SCPs is in the protocol.

The ISTP resides in the MGC, CMS, and SG. Figure 6 below shows the protocol stack model for ISTP within an IPCablecom SS7 Signaling Gateway.

ISTP requires a reliable underlying transport mechanism. The reliable transport will be provided by the Stream Control Transport Protocol (SCTP) [6] as defined in the IETF SIGTRAN working group. SCTP offers the following features:

- Explicit packet-oriented delivery (not stream-oriented).
- Sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages.
- Optional multiplexing of user messages into SCTP datagrams.
- Network-level fault tolerance through support of multi-homing at either or both ends of an association.
- Resistance to flooding and masquerade attacks.
- Data segmentation to conform to discovered path MTU size.

Note that it is the vendor and operator's responsibility to configure the selected stack and network to meet timing, reliability and security requirements for signaling. Appendix II documents how to use SCTP as the reliable transport for ISTP.

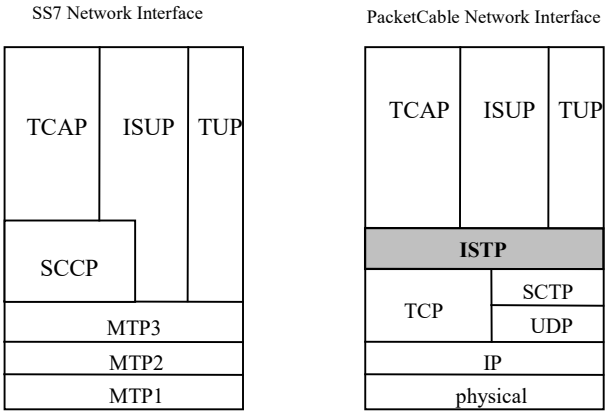

Figure 6. SS7 Signaling Gateway Protocol Stack Model using SCTP

7 FUNCTIONAL AREAS

The primary purpose of ISTP is to transport information from the SS7 network to the IPCablecom call control elements in a reliable and timely fashion over the managed IP network.

From the perspective of SS7 network elements, the Signaling Gateway looks like an SSP for incoming and outgoing SS7 messages. The SG will use information extracted from the SS7 stack and map that information to IP addresses in the IPCablecom network. It will then create an ISTP packet containing the signaling message data and ISTP header data, and send it to the selected node in the IPCablecom network.

From the IPCablecom IP network elements, the Signaling Gateway looks like any IP end node. The SG will take information from the ISTP header data and use it to map to SS7 addresses. It will then create an ISUP, TUP, or TCAP message and send it to the SS7 network.

Note: for the remaining discussion, comments on ISUP are automatically assumed to apply to TUP as well, so TUP will not be mentioned. Also note that IPCablecom does not currently specify the use of TUP for any features. It is mentioned in this document for completeness only.

7.1 Mapping Relationships

Some data structures are vital to the mapping and other functions of ISTP; they have global scope, and need to be consistently understood by all elements using ISTP. This mapping includes the basic numbering units for SS7 and IPCablecom networks: SS7 point codes, circuit identification codes, subsystem identity numbers, MGC identifiers, and IP addresses. In addition, ISTP adds a new numbering unit visible to ISTP nodes, the Circuit Identity (CID, pronounced "kid"). An SS7 trunk is identified by a Circuit Identification Code (CIC). The CIC is created by a negotiation between a gateway SS7 end-point node and a SS7 node at the "other end", and may be duplicated within a SG. Thus it does not uniquely identify a trunk. The CID, which is a combination of the IPCablecom gateway's ANSI point code and the Media Gateway's PSTN trunk connection to which it is assigned, allows the SG to uniquely identify an ISUP trunk circuit within the IPCablecom network. These identities are known by all ISTP elements and are exchanged in the activation and registration messages.

It is important to the understanding of the protocol for ISUP messages to realize that a set of CIDs, usually a trunk group, are allocated to one and only one MGC element (although the MGC itself can consist of multiple redundant MGCN nodes). Thus all ISUP messages containing CICs are routed over one of the multiple IP connections between the SG and the MGC element which controls that CIC.

Since trunks are fixed in the SS7 network and the MG, and CID's identify a trunk, the CID is a "hard" identification of a network resource terminated on a single MG and controlled by a single MGC. However, since trunks are usually allocated in groups of 24 circuits in a T1, a *range* (usually multiples of 24) of sequentially numbered circuits would typically be used in allocation and provisioning messages.

The mapping between the SG and CMS for TCAP messages is much more dynamic. TCAP uses fixed subsystem identities to determine routing to application types. Transaction identities are allocated dynamically by the transaction originator and can be used as the basis for a dynamic mapping mechanism in the SG. Thus, when an IPCablecom element, such as a CMS, originates a TCAP transaction, it will assign a unique ID to the transaction by populating the four-byte ISTP TCAP Transaction ID field. The originating element needs to guarantee that the transaction ID is unique for the life of the transaction within the scope of the originating element. However, because the Signaling Gateway receives TCAP queries from multiple IPCablecom elements, there is no guarantee that two or more elements will not use the same ISTP TCAP Transaction IDs at the same time. Therefore, to meet the uniqueness requirements of SS7 TCAP, the Signaling Gateway will create and manage new TCAP Transaction IDs for the outgoing queries to the SS7 network, according to the rules of SS7, and populate the SS7 fields appropriately. A unique mapping is thus created between the SS7 Transaction ID and the combination of the ISTP Transaction ID and the IPCablecom naming identifier for the originating element.

The Signaling Gateway will use this mapping relationship to correctly route TCAP responses from the SS7 network to the IPCablecom element that originated the query and MUST correctly populate the ISTP Transaction ID field in the response message to match that of the original query message.

7.1.1 SS7 Numbering

An ISUP message has a header portion and a parameters portion. In the header are the following:

- Trunk Circuit Identification Code (CIC), a two octet field that identifies the specific trunk circuits used to establish the voice or data connection path. This maps to a specific channel on a specific IPCablecom MG trunk, and is only changed by configuration of the network.
- Signaling Link Selection (SLS) code, not needed by ISTP.
- Origination Point Code (OPC), and Destination Point Code (DPC). These are unique SS7 network addresses that identify the message origination or destination signaling point. In ANSI, the network is zoned into three components: the Network, Network Cluster, and Network Cluster Member. Each represents a hierarchical number in the network address, and together identifies a unique signaling point (an SSP or STP or Intelligent Peripheral). Each component is a byte. ITU defines three similar components (named differently) with 3 bit, 8 bit, and 3 bit components.

A TCAP message contains a Component portion and a Transaction portion. The Transaction portion contains:

- TCAP packet type, describing the nature of the request. It contains the data necessary to relate the message to other messages, which can be part of the same transaction. This is not used by ISTP.
- TCAP message length.
- Transaction ID identifier.
- Transaction ID length.
- Transaction ID, (TID) which uniquely identifies the transaction. The originator of the message usually provides it, although there are cases where the receiver can create a TID.
- Component sequence identifier, which indicates the sequence of components to follow.
- Component sequence length.
- Component type identifier.

7.1.2 IPCablecom Numbering

Media Gateway Controller names are encoded as e-mail addresses as defined in RFC 821. In these addresses, the domain name identifies the system where the MGC is attached.

Both components MUST be case insensitive.

Refer to the IPCablecom Network Call Signaling Protocol Specification [16] for more details.

An example of MGC name is:

MGC@mgc.whatever.net Media Gateway Controller for the "whatever" network.

Reliability is provided by the following precautions:

- Media Gateway Controllers are identified by their domain name, not their network addresses. Several addresses can be associated with a domain name.
- If a command cannot be forwarded to one of the network addresses, implementations MUST retry the transmission using another address.
- Entities can move to another platform. The association between a logical name (domain name) and the actual platform are kept in the Domain Name Service (DNS). To provide fast reliable access, ISTP elements maintain IP address mapping in internal SG tables as well. These configuration tables are updated by vendor dependent mechanisms, and need to be kept current with the DNS values.

Nodes in the IPCablecom IP network are currently identified by IPv4 addresses (a.b.c.d.) as per RFC 791 [4].

7.1.3 ISTP Numbering

ISUP (ISDN User Part) messages rely on CICs (Circuit Identification Code) to process calls in the PSTN environment. The CIC is the actual circuit trunk connection between switches, usually CLASS IV Tandem switches and can range from number from 1 to 16,333 with a least significant octet and a most significant octet comprising the number. This numbering identifies the circuit being reserved, in use or being disconnected and usually rides a DS1 (24 trunks) circuit between to switching points. In IPCablecom gateways, the Media Gateway Controller relies on the CID. The CID is the actual connection for the Media Gateway to the PSTN. Thus, one can state that the CID is a combination of the gateway's ANSI point code and PSTN trunk (CIC).

TCAP queries are identified by a transaction ID. The CMS shall create and use the ISTP Transaction identity. The SG shall map the ISTP transaction identity to a SS7 transaction identity as defined per the relevant TCAP standards. Transaction identities are kept only for a length of time much greater than the longest TCAP transaction.

7.2 Message Distribution

ISUP messages destined to the MGCs are routed from SS7 to ISTP elements by mapping the CID to an IP address associated with the corresponding MGC node. TCAP queries from the CMS or MGC are routed by mapping a transaction id to an originating IP address; TCAP responses are returned in the same manner.

Some messages are internal to ISTP and are routed by IP messaging to all ISTP nodes sharing a point code. This includes maintenance messages, configuration messages, and congestion messages.

7.3 Mapping

One function of the ISTP is to map the target address between the SS7 and IP based IPCablecom networks for ISUP messages. From the SS7 network, given a CIC, a DPC and an OPC in an incoming SS7 network ISUP message, it will find a target MGC element name of a target MGC element, then find the MGC Node's IP address or SCTP association from an ordered list of MGC Nodes and forward the message to the selected MGC node. From the IP network, given a target point code in an outgoing MGC ISUP message, it will forward the message to the SS7 network.

For TCAP messages, a similar mapping is required. For queries initiated from the IP network, given a TCAP transaction portion and an MGC name and IP address of the node initiating the transaction, ISTP will forward the TCAP message to the targetpoint code, and return replies to the correct sender. This mapping is dynamic, and only kept for the length of the transaction, which is known from the TCAP packet type. A second function of ISTP is to re-map to redundant or alternate paths upon detection of communication failures. On failures or communication timeouts:

- If a MGC/CMS IP communication fails, it will look up alternate IP addresses first for that MGC/CMS element.
- If a SG IP communication fails, the MGC/CMS will look up alternate IP addresses to the SG element.

Given the performance requirements, ISTP SHOULD avoid using IP addresses that are known to be unavailable, that is, are out of service or have failed a heartbeat test and timed out. Timers should be based on the specifications of the TCAP retransmission timers of the interfacing network. (ANSI based network are in the order of 30 secs.)

7.4 Relationships

To support the necessary mapping and distribution functions, ISTP assumes a set of relationships. These relationships will typically be in a database and administered by the operations staff. They include:

- CID to MGC: this maps a range of CIDs (representing channels in trunks) to a single MGC element name.
- MGC to IP: this maps an MGC element name to one or more MGC nodes, identified by IP addresses.
- SG to IP: this maps the SG element, identified by its point code, to one or mode SG nodes, identified by an IP address.

IP status: this keeps the current availability status of a IP node so that the ISTP will select a working IP address only, and prevent the selection of unavailable IP addresses which would cause a timeout.

7.5 Initialization

The ISTP initialization MUST handle the following scenarios:

- Complete "cold start" initialization of all elements, communications, and dynamic data in all the nodes of the IPCablecom network.
- CMS element initialization, which initializes all IP physical and logical communications as well as all ISTP data in the CMS element and its node in the IP network.
- MGC element initialization, which initializes all IP physical and logical communications as well as all ISTP data in the MGC element and its nodes in the IP network.
- SG element initialization, which initializes all IP physical and logical communications as well as all ISTP data in the SG element and its nodes in the IP network.
- CMS single node initialization, which initializes the node's IP physical and logical communications as well as ISTP data.
- MGC single node initialization, which initializes the node's IP physical and logical communications as well as ISTP data.
- SG single node initialization, which initializes the node's IP physical and logical communications as well as ISTP data.
- ISTP only initialization, which initializes ISTP data.
- IP communication only initialization, which initializes all IP physical and logical communications, as well as all affected ISTP configuration.

When an ISTP stack restarts, it needs to be given all necessary information (e.g.: point code identity, MGC/CMS/SG lists, CIC range, IP identities); how this is achieved is left to the specific implementation.

When a new CIC range, CIC, MGC/CMS identity, IP address, or SG point code is added to the network, all ISTP nodes sharing a common point code in the MGC-SG network need to be informed and given the new or revised mapping in a consistent fashion by the trunking gateway operations support system.

When an element or node restarts, it should notify the all other known ISTP nodes sharing a common point code using the SS7 network inaccessible message and the SS7 network accessible messages when it is back in service; this shall be done in an orderly manner so that it will not flood a node or network after an outage.

7.6 Recovery

Given the PSTN-like or higher availability requirements, the ISTP needs to recover from failures quickly and robustly. ISTP is designed to handle fully distributed n+k node architecture for the IPCablecom IP network, as well as interface to the various SS7 highly reliable network configurations.

At the physical Level, the ISTP MUST manage two or more network level interfaces to the IP systems. In the event of a failure of one of the IP interfaces it should switch over to another IP interface.

At the IP node level, each IP communication must be addressable from either of the physical network interfaces. While ISTP makes no assumptions on the recovery capabilities implemented by the MGC element, it will assume the best case and expect the MGC to have advanced recovery features that can recover active communications in the event of a single MGC node failure. Thus, if a far end IP interface on a MGC or SG fails, the ISTP MUST try a second IP address; if this fails a third should be tried, etc., up to the optionally provisioned limit of the IP signaling network. Before trying any IP address, the ISTP should check its availability status. If the MGC element can not recover a communication, the SG will discard the messages only after trying all MGC nodes and failing to establish communication.

At the MGC/SG level, each MGC element needs to be addressable from the SG. If one MGC fails, it is again assumed that a redundant MGC can possibly recover the communication, and the ISTP MUST retry to a second MGG; if this fails a third should be tried, etc., up to the optionally provisioned limit of the IPCablecom IP signaling network. Again, if the MGC element can not recover the communication, the SG will discard the messages only after trying all MGC nodes and failing to establish communication.

There is only one SG (comprised of possibly multiple IP nodes). If it fails, recovery is beyond the scope of the ISTP, and the MGC needs to take recovery actions.

7.7 Dynamic Provisioning

The ISTP internal configuration mapping relationships MUST be dynamically updated without a network restart. Any vendor can store information in a local database, or require a central distribution of data on node recovery: this is an implementation option.

The operational support system for the ISTP needs to have an audit feature that will allow network management to validate a successful configuration. This will be done using OA&M functions whose definition is beyond the scope of this document.

Changing a mapping relationship needs to be done in a graceful and consistent manner across the entire IPCablecom network. Thus administration of ISTP data MUST be implemented in the following way.

- For changes to existing relationships the entire IPCablecom network needs to be changed as one consistent transaction.
- For any change to a relationship the addressable IP nodes need to be managed in a graceful fashion; each node need to first be disabled (put out of service), then configured, audited to verify correct configuration, and then enabled (put back in service) in a way that does not suddenly flood the network.

For new relationships, there is no IP node to disable, but the provision needs to also be handled as one consistent transaction, audited, and each node placed in service gracefully.

7.8 Administration

The ISTP defines some semi-permanent objects and relationship (e.g., timers) that need to be administered by the service provider's operations staff. The mechanisms and processes used to administer this data and behavior are currently beyond the scope of this document.

7.9 Security

Message authentication will use current state of the art Intranet technology to ensure safe and secure transport of IP messaging. Any further security required at ISTP and higher level will result from the efforts of a separate IPCablecom group dedicated to the issue, and is currently beyond the scope of this protocol specification.

7.10 Maintenance

ISTP manages the IP communications owned by the particular MGC, SG, or CMS, so it can proactively skip failed IP addresses when searching for a target IP without waiting for a timeout. It supports the following procedures:

- Enable IP, which places the IP connect in service and allows traffic.
- Disable IP, which removes the IP connection form service.
- Wait for traffic clear on IP connection.
- Restart IP connection.

The operations support system will supply interfaces for these procedures to allow operations staff to manually manage the IP address states. For autonomous recovery, messages for these procedures need to be defined.

Note that the ISTP does not specify element or node management, only IP communications management. Management of the element or nodes involved many more functions than handled by ISTP. These functions will by handled by the OSS and their definition is beyond the scope of this document.

ISTP provides no additional requirements on SS7 maintenance.

7.11 Measurement

Operational measurements will be collected; the details on these issues are currently beyond the scope of this protocol specification.

7.12 Alarms

At a minimum the ISTP should generate alarms whenever an IP connection fails and whenever an ISTP node restarts.

7.13 Congestion

Congestion on the SS7 network will be handled as per SS7 specifications on the interfacing PSTN network. This means that the CMS and the MGC need to handle congestion messages from the SG and meet the SS7 requirements in this area. The ISTP will only pass congestion messages to the CMS and MGC; the SG itself will only take SCCP/MTP level recovery actions.

7.14 Management of Lower Layers

ISTP uses SCTP or TCP as its transport layer protocol and must manage the SCTP associations. Refer to Appendix II for SCTP or TCP usage recommendations.

The SG manages the lower layers of SS7 stack. When the status of lower layer objects, like nodes, network clusters, or subsystems, change, SG is responsible for reporting the changes to MGC. MGC should respond to the status changes according to the SS7 specification of the interfacing network.

8 PROTOCOL

8.1 General Requirements

The ISTP protocol is in essence a translation of the MTP and SCCP primitives between the transport and application layers of the SS7 protocol to work over a distributed IP network. It presents a subset of the MTP SS7 level functionality to applications in the IP network. These include:

- A message distribution function that distributes ISUP and TCAP messages to/from distributed signaling components on the IP network. (This is done in lieu of the route-sets and link-sets of the SS7 network.)
- An encoding schema for the transport of SS7 messages over a reliable IP-based protocol.
- A set of messages and procedures for dynamically configuring the ITSP network on the IP side.

8.1.1 Communication with the Lower Layers

The ISTP protocol does not have specific procedures for the dynamic establishment and the closure of connections between the MGC/CMS and the SG. It relies on a connection-oriented interface with the lower layers established at initialization or configuration time to:

- Establish a reliable communication path.
- Guarantee the prompt and sequenced delivery of the messages.
- Provide information about the origination of incoming messages.
- Retransmit messages in case of errors or timeouts.
- Promptly detect failures in the communication path.
- Close communications.

ISTP is designed to use either TCP or SCTP as its lower layer. When using SCTP, the SG is considered to be the server. The MGC nodes and CMS nodes must initiate the connection to the SG.

The procedures for the setup and takedown of the TCP or SCTP connections are defined in Appendix I.

8.1.2 Encoding Rules

ISTP messages use an 8-bit binary encoding scheme referred to as "octet", due to the nature of SS7 messages, as defined by ANSI. The content and the encoding of all parameters used in ISTP are defined in this document, except for the content of the ISUP and TCAP parameters.

The content of the signaling messages is exchanged between the MGC and the SG in one of two formats: raw format or normalized format.

Raw format means a message that is the exact SS7 message given to the SG by the network; normalized format means a message that may have certain parameters or formats modified by the SG to present a common format in cases where the SS7 network protocol uses a variant of a standard.

When using raw formatting, the content of the SS7 message is conveyed in its native MTP form, as outlined by the ANSI specification. The SS7 message is transferred to the Media Gateway Controller using normalized formatting.

8.1.3 SS7 Load-Sharing and Sequencing

In a conventional SS7 application, the MTP Level 3 relies on the upper layers to supply the signaling link selection (SLS) value for each message to be transferred to the SS7 Network. The MTP Level 3 uses this value to distribute the traffic evenly between available signaling links, but expects an even distribution of the SLS values in order to achieve balanced load on all links.

The MTP Level 3 also ensures the sequenced delivery of messages to the destination for a given SLS.

In the ISTP protocol, it is the responsibility of the SG to assign the SLS value based on the CIC or the Transaction ID for outgoing messages in order to ensure optimal SS7 performance.

8.2 Procedures

8.2.1 Registration of Circuit Identifiers

In order to send and receive ISUP messages for a given circuit, the MGC MUST register the circuits it manages with the SG. Registration of circuit identifiers is required for the SG to:

- Properly distribute ISUP messages received from the SS7 network. The SG has an elaborated MSU distribution function which uses the DPC, OPC and CIC for ISUP messages.
- Provide some validation of the MSUs bound for the SS7 network.

Once an MGC is successfully registered, it needs to activate the entries in order for them to take effect. In essence, the registration is a validation step meant to minimize conflicting MGC entries, whereas the activation procedure is the one actually having an effect on the distribution of traffic.

Only one MGC element may be registered on a given circuit. Redundancy is achieved by having more than one MGC node within an MGC element to register with more than one SG node. MGC elements are identified by name.

The SG MUST deny attempts to register more than one MGC element on a given circuit.

MGC nodes do not have a unique identifier. Their IP interfaces are identified by their IP addresses. The ISTP protocol does not differentiate between IP interfaces belonging to one MGC node, or belonging to multiple MGC nodes.

8.2.1.1 Circuit Registration

The MGC node sends a circuit registration request to the SG node to reserve the specified circuit range. It also specifies, in the message, the requested transfer format; whether it wishes to receive the raw ISUP message parameter or the normalized ISUP message parameter. Parameters to the registration request include the MGC name, the gateway point code, the target point code, the CIC range, and the message format.

When a SG node receives a circuit registration request, it verifies that:

- It can locally service the gateway point code (i.e. it is the local point code of the SG element).
- It has access the target point code using its provisioned SS7 routing tables.
- The point codes and CIC range parameters contain valid values for the requesting MGC node in its authentication tables.
- No other MGC element has successfully registered with requested circuit. This verification is made by ensuring that the provided MGC name is consistent with the currently registered MGC nodes for the given circuit, if any, on all SG nodes.
- It can support the requested message format.

If the SG node determines that the circuit registration request is acceptable, it sends a circuit registration acknowledgement to the requesting MGC node with a success indication. If it determines that it cannot grant the registration, it returns an acknowledgement with the proper failure indication.

The authentication tables and algorithms are implementation dependent.

8.2.1.2 Circuit De-Registration

The MGC node sends a circuit de-registration request to the SG node to indicate that it no longer wishes to reserve the specified circuit range. Parameters of the de-registration request include the MGC name, the gateway point code, the target point code and a CIC range.

When the SG node receives a circuit de-registration request, it verifies that the circuit(s) are currently registered with the requesting MGC. If the circuit(s) are registered with the SG node, it responds with a circuit de-registration acknowledgement with a success indication. If not, it returns an acknowledgement with the proper failure indication.

8.2.2 Activation of Registered Circuits

Once the MGC node has been properly registered, it needs to activate the registered entries in order to allow the flow of ISUP messages between the MGC node and the SS7 network.

More than one registered MGC node can be active for the same circuit(s). The method of message distribution to multiple active MGC nodes is implementation dependent.

8.2.2.1 Circuit Activation

The MGC node sends a circuit activation request to the SG node when it wishes to send and receive SS7 messages pertaining to the specified circuits. Some parameters include the MGC name, DPC, OPC and CIC range.

When the SG node receives a circuit activation request, it verifies that:

- The MGC node has successfully registered the circuit range prior to receiving this request.
- The MGC node is not already active for the given circuit(s).

If the SG node determines that the circuit activation request is acceptable, it sends a circuit activation acknowledgement to the requesting MGC node with a success indication, and starts allowing message transfer with the requesting MGC node for the specified circuit(s). It uses an implementation-dependent message distribution algorithm if one or more MGC node was already active for the specified circuit(s).

If the SG node determines that it cannot grant the activation, it returns an acknowledgement with the proper failure indication.

8.2.2.2 Forced Exclusive Circuit Activation

The MGC node sends a forced exclusive circuit activation request to the SG node when it wishes to send and receive SS7 messages pertaining to the specified circuits, and override any existing activation(s) for the SG node. The parameters include the MGC name, the gateway point code, the target point code and CIC range.

When the SG node receives a forced exclusive circuit activation request, it verifies that the MGC node has successfully registered the circuit range prior to receiving this request.

If the SG node determines that the forced exclusive circuit activation request is acceptable, it sends a forced exclusive circuit activation acknowledgement to the requesting MGC node with a success indication. It starts allowing message transfer for the specified circuit(s) exclusively with the requesting MGC node. It also sends a forced circuit deactivation indication to any previously active MGC node(s) for the specified circuit(s), and stops message transfer for the specified circuit(s) on all previously active MGC nodes.

An already active MGC node can also request exclusive circuit activation.

If it determines that it cannot grant the exclusive activation, it returns an acknowledgement with the proper failure indication.

This procedure is meant to facilitate the recovery service in the event of failed MGC nodes. It can be used to take over failed nodes or any other activity that requires forced exclusive activation of circuits.

The exclusivity status of the circuit activation is not permanent. Once the exclusive activation procedure is completed, other MGC nodes can successfully activate the same circuit(s).

8.2.2.3 New Work Circuit Activation

The MGC node sends a new work circuit activation request to the SG node when it wishes to send and receive SS7 message concerning new work on the specified circuits, complementing any existing activation(s). This procedure is used when work needs to be gracefully moved over from one or more MGC nodes to another. Some parameters include the MGC name, DPC, OPC and CIC range.

When the SG node receives a new work circuit activation request, it verifies that the MGC node has successfully registered the circuit range prior to receiving this request, and that the requesting MGC node is not already active.

If the SG node determines that the new work circuit activation request is acceptable, it sends a new work circuit activation acknowledgement to the requesting MGC node with a success indication. It also sends a new work circuit deactivation notification to any previously fully active MGC node(s) for the specified circuit(s). It then starts diverting new work traffic to the newly activated MGC, and continues sending work in progress to the previously active MGC(s). If two or more MGC nodes were successfully activated for new work on a specific circuit, then the ISUP messages pertaining to the circuit are distributed to the MGC nodes using an implementation-dependent message distribution function.

If there was no previously active MGC node for the specified circuit, the new work circuit activation is treated like a normal circuit activation request, and a circuit activation response is sent as an acknowledgement instead of the new work circuit activation response.

If the SG node determines that it cannot grant the new work circuit activation, it returns an acknowledgement with the proper failure indication.

Once the MGC node determines that it wishes to receive all the traffic, it can use the exclusive activation procedure to divert all the traffic to it, or alternatively, the previously active MGC nodes can terminate their active status by sending a circuit deactivation request to the SG node(s).

8.2.2.4 Circuit De-Activation

The MGC node sends a circuit de-activation request to the SG node to indicate that it no longer wishes to send or receive messages pertaining to the specified circuits. Parameters of the de-activation request also include the MGC name, DPC, the OPC and a CIC range.

When the SG node receives a circuit de-activation request, it verifies that the circuit(s) are currently active for the requesting MGC node. If the circuit(s) are active for the MGC node, it responds with a circuit de-activation acknowledgement with a success indication and promptly stops to transfer messages relating to the specified circuits for the requesting MGC node. If not, it returns an acknowledgement with the proper failure indication.

8.2.3 Registration of Subsystem Transactions

In order to exchange TCAP messages with nodes in the SS7 network; the CMS/CA MUST properly register with the SG. Registration is required for the SG to:

- Properly distribute MSUs received from the SS7 network. The SG has an elaborated MSU distribution function which uses the gateway point code and SSN for TCAP messages;
- Provide some validation of the MSUs bound for the SS7 network.

A CMS/CA element registers with the SG as a subsystem. Subsystems are identified by the local point code of the SG and by the subsystem number (SSN) of the CMS/CA. This allows responses to CMS/CA initiated transactions to be returned to the CMS/CA on point code and subsystem number basis as specified in the initiating party's address. This also allows PSTN initiated transactions and unidirectional messages to be routed to the CMS/CA element.

Once an application is successfully registered, it needs to activate the entries in order for them to take effect. In essence, the registration is a validation step meant to minimize conflicting CMS/CA entries, whereas the activation procedure is the one actually having an effect on the distribution of traffic.

Multiple CMS/CA nodes can be registered with the same gateway point code and SSN values, and more than one can be active at any given time. Only one CMS/CA element can be registered with a SG element for the same point code and SSN values. The SG MUST deny attempts to register more than one CMS/CA element on a given subsystem.

8.2.3.1 Subsystem Registration

The CMS/CA node sends a subsystem registration request to the SG node to reserve the specified subsystem. It also specifies, in the message, the requested transfer format; whether it wishes to receive the raw TCAP message

parameter or the normalized TCAP message parameter. Parameters to the registration request include the gateway point code, the SSN and the message format.

When the SG node receives a subsystem registration request, it verifies that:

- It can locally service the gateway point code (i.e. it is the local point code of the SG).
- It can locally service the subsystem as specified in the SSN field.
- The point code and SSN parameters contain valid values for the requesting CMS/CA in its authentication tables.
- No other CMS element is registered with the SG element for the given point code and SSN values.
- It can support the requested transfer format.

If the SG node determines that the subsystem registration request is acceptable, it sends a subsystem registration acknowledgement to the requesting CMS node with a success indication. If it determines that it cannot grant the registration, it returns an acknowledgement with the proper failure indication.

8.2.3.2 Subsystem Transaction De-Registration

The CMS node sends a subsystem de-registration request to the SG to indicate that it no longer wishes to reserve the specified subsystem. Parameters of the de-registration request also include the DPC, the OPC and the SSN.

When the SG receives a subsystem de-registration request, it verifies that the subsystem is currently registered with the requesting CMS node. If the subsystem is registered with the SG node, it responds with a subsystem de-registration acknowledgement with a success indication. If not, it returns an acknowledgement with the proper failure indication.

8.2.4 Activation of Registered Subsystem Transactions

Once the CMS node has been properly registered, it needs to activate the registered entries in order to allow the flow of SCCP messages for the specified subsystems.

There are no procedures defined for maintaining work in progress transactions with the specific CMS nodes. Most TCAP transactions have a very short life, and the implementation of new work activation messages would add unnecessary complexity to ISTP.

8.2.4.1 Subsystem Activation

The CMS/CA sends a subsystem activation request to the SG node when it wishes to send and receive SS7 messages pertaining to the specified subsystems. Parameters include the gateway point code and SSN.

When the SG node receives a subsystem activation request, it verifies that:

- The CMS/CA node has successfully registered the subsystem prior to receiving this request.
- The CMS/CA node is not already active for the requested subsystem.

If the SG node determines that the subsystem activation request is acceptable, it sends a subsystem activation acknowledgement to the requesting CMS/CA node with a success indication, and starts allowing message transfer with the requesting CMS/CA node for the specified subsystem.

If more than one CMS/CA node is active for the same subsystem, the TCAP messages are distributed to the CMS/CA nodes using an implementation dependent distribution algorithm for queries and unidirectional messages coming from the SS7 network.

If the TCAP message coming from the SS7 network is a response or a conversation message pertinent to an earlier request by one of the CMS/CA nodes, then the message is sent to the requesting CMS/CA node. The selection of the originating CMS/CA node is done at the SG element by keeping a dynamic list of the originating transaction IDs, and by correlating the responding transaction ID of the incoming message with that dynamic list.

If the SG node determines that it cannot grant the activation, it returns an acknowledgement with the proper failure indication.

8.2.4.2 Forced Exclusive Subsystem Activation

The CMS node sends a forced exclusive subsystem activation request to the SG node when it wishes to send and receive SS7 messages pertaining to the specified subsystem on an exclusivity basis, and override any existing activation. Some parameters include the DPC, OPC and SSN.

When the SG node receives a forced exclusive subsystem activation request, it verifies that the CMS node has successfully registered the subsystem prior to receiving this request.

If the SG node determines that the forced exclusive subsystem activation request is acceptable, it sends a forced exclusive subsystem activation acknowledgement to the requesting CMS node with a success indication. It starts allowing message transfer with the requesting CMS node for the specified subsystem. It also sends a forced subsystem deactivation indication to any previously active CMS node(s) for the specified subsystem, and stops message transfer for the specified subsystem on all previously active CMS nodes.

If it determines that it cannot grant the exclusive activation, it returns an acknowledgement with the proper failure indication.

8.2.4.3 Subsystem De-Activation

The CMS/CA node sends a subsystem deactivation request to the SG node to indicate that it no longer wishes to send or receive messages pertaining to the specified subsystem. Parameters of the de-activation request also include the DPC, the OPC and the subsystem.

When the SG node receives a subsystem de-activation request, it verifies that the subsystem is currently active for the requesting CMS/CA node. If the subsystem is active for the CMS/CA node, it responds with a subsystem de-activation acknowledgement with a success indication and promptly stops to transfer messages relating to the specified subsystem. If not, it returns an acknowledgement with the proper failure indication.

8.2.5 Message Transfer

The message transfer procedure is the one by which the MGC, then CMS/CA and the SG exchange SS7 messages back and forth. The MGC or the CMS/CA sends a message transfer indication to the SG to send an SS7 message to the specified destination. The SG sends a message transfer indication to the MGC or the CMS/CA when it receives a message from the SS7 network for which the registered element has an interest.

8.2.5.1 ISUP Message Transfer

The SG sends an ISUP message transfer indication to the MGC when it receives an ISUP MSU that has a matching point code, target point code and CIC with one of the activated entries for the MGC.

The MGC sends an ISUP message transfer indication to the SG to send an ISUP message to the specified destination.

8.2.5.2 TCAP Message Transfer

The CMS/CA sends a TCAP message transfer indication to the SG to send a TCAP message to the specified destination.

When the SG receives an MSU with a service indicator value of 3 (SCCP), it gets processed through the SCCP portion of the enhanced distribution function.

If the message type is not a UNIT-DATA or UNIT-DATA-SERVICE or is an SCCP management message, it is handled by the SG. If the message type is a UNIT-DATA or a UNIT-DATA-SERVICE carrying TCAP information the message is routed to the appropriate CMS node in a TCAP message transfer indication. The routing is based on the DPC, the SSN and the Transaction ID.

There are two types of transaction identifiers that concern ISTP elements. There are the TCAP transaction IDs, which are defined in various SS7 standards. TCAP messages contain either an originating ID, a responding ID, both or none, depending on the TCAP message type. These transaction identifiers are defined to be unique for the duration of the transaction between the SS7 nodes.

There is also a transaction identifier used between ISTP elements. This transaction identifier is unique between the CMS/CA element and the SG element for the duration of the transaction. This transaction identifier is defined by the CMS/CA at the moment of a launch a query or of a conversation message.

When the CMS/CA sends a query message to the SG using the TCAP message transfer procedure, the ISTP transaction ID is set to a unique value as defined by the CMS/CA, and the TCAP originating transaction ID is set to zero. When the SG receives this message, it creates a unique TCAP originating transaction ID and stores it in the TCAP message before sending it to its SS7 destination. The SG also takes note of the originating CMS/CA node's IP address and ISTP transaction ID, in order to send the response to the appropriate IP destination. The same action is taken for conversation messages, except that the TCAP responding transaction ID is set to the TCAP originating transaction ID of the incoming query or conversation message.

When the CMS/CA sends a response or a unidirectional message to the SG, no special routing based on the transaction ID is required.

When the SG receives a query or a conversation message from the SS7 network, it extracts the TCAP responding transaction ID and matches it with the ISTP transaction ID previously set by the CMS for the current transaction. It then forwards the MSU using the TCAP Message Transfer format to the appropriate CMS node using the previously saved information.

When the SG receives a query or a unidirectional message from the SS7 network, it sends TCAP Message Transfer to an active CMS node, which is selected using an implementation dependent algorithm.

In all instances, TCAP Message Transfer can be only exchanged for currently active subsystems.

8.3 Failure Detection and Handling

There are some conditions that can prevent the proper flow of messages between the MGC and SG. These conditions include:

- The inability of the SG to transfer a message received from the MGC or a CMS onto the SS7 network.
- The inability of the SG to transfer a message received from the SS7 network to an MGC or a CMS.
- The loss of connectivity of the SG to the SS7 network.
- The loss of connectivity between the MGC or a CMS and the SG.
- The detection of congestion on the SS7 network.
- The detection of congestion on the IP network.

8.3.1 Heartbeat

The ISTP elements can lose connectivity or a processing module that can remain undetected by the lower communication layers. In order to minimize the impact of such an event, ISTP has a heartbeat procedure that is implemented by all ISTP nodes.

This procedure functions on a query-response basis. When an ISTP node wants to question the validity of a connection, it sends a heartbeat request, and expects the receiving end to promptly respond with a heartbeat response. All ISTP nodes MUST send heartbeat requests on a periodic basis, and must respond to incoming heartbeat requests as soon as they are received.

When ISTP is running on top of TCP, the heartbeat is used to detect IP connection failure and congestion before trying to send messages. It is also used to detect application module failures. When ISTP is running on top of SCTP, the heartbeat use only used to detect application module failures, since SCTP will recognize IP connection anomalies. The detailed steps taken upon delayed or missing heartbeat responses are implementation dependent, but failed IP connections should be disabled within a time period that allows the IPCablecom network to meet its stated availability requirements.

8.3.2 Signaling Gateway Procedures

8.3.2.1 Signaling Point Accessibility

The SG can lose access to SS7 signaling point due to local SS7 link failures, remote routing failures, or maintenance activities.

If the SG loses connectivity to a SS7 signaling point for which there is a concerned MGC or a concerned CMS (i.e., MGCs that have registered circuits that terminated on the affected signaling point), it sends a signaling point inaccessible indication to each concerned MGC and CMS node. According to the SS7 specifications, it also stops transferring messages from the MGC or the CMS to the affected signaling point, and discards messages bound to the unavailable signaling point.

If a signaling point becomes accessible and there is a concerned MGC or CMS, the signaling gateway sends a signaling point accessible indication to each concerned MGC and CMS node. It also resumes the transfer of messages to the affected signaling point and to all concerned MGCs and CMSes.

8.3.2.2 Subsystem Accessibility

The SG can lose access to an SCCP subsystem due to remote SCP failures or maintenance activities.

If the SG loses connectivity to a subsystem signaling point for which there is a concerned CMS (i.e. CMSes that have registered subsystem with the affected signaling point), it sends a subsystem inaccessible indication to each concerned CMS node. According to the SS7 specifications, it also stops transferring messages from the CMS to the affected subsystem.

If a subsystem becomes accessible and there are some concerned CMSes, the signaling gateway sends a subsystem accessible indication to each concerned CMS node. It also resumes the transfer of messages to the affected subsystem and to all concerned CMSes.

8.3.2.3 SS7 Network Accessibility

The SG can also lose complete accessibility to the SS7 due to the failure of all local SS7 links. When this occurs, the SG sends a SS7 network inaccessible indication to all connected ISTP nodes. At this point it also stops accepting all messages being transferred to the SS7 by discarding them.

When the SG gains access to the SS7 network because of SS7 link restoration, it waits for the MTP-Restart procedure to complete (see respective SS7 standards), then sends a SS7 network accessible indication to all connected ISTP nodes. At this point it resumes the transfer of SS7 messages and of ISTP transfer messages.

8.3.2.4 MGC/CMS Accessibility

The SG can lose connectivity to an MGC or a CMS because of IP network or node failures, or scheduled maintenance. When the SG detects loss of connectivity to a ISTP node it de-activates and de-registers all circuits and subsystems with that ISTP element, and discards any subsequent SS7 message are not claimed by any ISTP node.

It is the responsibility of the MGC and the CMS to re-establish connectivity or to arrange for alternate MGC(s) or CMS(s) to register and activate the affected circuits and subsystems.

When an MGC or a CMS re-establishes connectivity with the SG, it uses the normal registration and activation procedures.

8.3.2.5 Congestion on the SS7 Network

If the SG detects the congestion of a signaling point by receiving a TFC message, it sends a signaling point congestion indication to the concerned MGC and CMS nodes with the congestion level that was received in the original TFC message.

The SG should provide a mechanism for detection of the end of a congestion status. In this case, it sends a signaling point congestion indication to the concerned MGC and CMS nodes with a congestion level of 0.

If the SG detects congestion of the local SS7 links for outbound traffic, it sends a local congestion indication to all connected MGC and CMS nodes with an appropriate congestion level. When the congestion status ends, the SG sends a local congestion indication to all connected MGC and CMS nodes with a congestion level of 0.

8.3.2.6 Congestion on the IP Network

If the SG detects congestion of the IP network to the MGC or the CMS node, it does not notify the adjacent SS7 nodes. Instead, it uses a four level congestion scheme as defined in ANSI MTP level 3, and discards messages based on the priority of the messages as defined in the service information octet. If the message priority information is not available (i.e., ITU networks), messages are discarded using the local congestion rules.

The method of detection and the measurement of congestion on the IP network is defendant on the lower layer used, and on the implementation.

8.3.3 MGC and CMS Procedures

8.3.3.1 Signaling Point Accessibility

When a concerned MGC or CMS node receives a signaling point inaccessible indication, it treats this message as an MTP-PAUSE primitive as defined in the various SS7 standards. It marks that destination as inaccessible, and stops transferring messages to the signaling gateway destined to the affected signaling point.

When a concerned MGC or CMS node receives a signaling point accessible indication, it treats this message as an MTP-RESUME primitive as defined in the various SS7 standards. It marks the destination as accessible, and resumes transferring messages to the signaling gateway destined to the now accessible signaling point.

8.3.3.2 SS7 Network Accessibility

When an MGC or CMS node receives a SS7 network inaccessible indication, it stops all message transfer to the SG.

At this point the SG is no longer in a position to be informed about the accessibility of other signaling points.

When an MGC or CMS node receives a SS7 network accessible indication, it assumes that all destinations are available until told otherwise. It also resumes the transfer of messages to and from the SG.

8.3.3.3 Signaling Gateway Accessibility

When an MGC or CMS node loses connectivity to the SG, active circuits and subsystem transactions are automatically deactivated. All registered circuits and subsystems are also de-registered.

If the MGC or CMS node was providing service for some circuits or subsystem transactions, it tries to re-establish service to minimize the downtime associated with the failure. It can accomplish that by requesting backup from an alternate system, and by attempting to re-establish the connection with the SG.

The specific recovery procedures are implementation specific.

8.3.3.4 SS7 Network Congestion

When an MGC or CMS node receives a signaling point congestion indication, it marks the destination as congested with specified level. It also treats this message as an MTP-STATUS with congestion level primitive as defined in the various SS7 standards.

If the congestion level is non-zero, it applies the proper message throttling and filtering algorithms to the affected destination in order to alleviate the congestion status and to prevent undesirable message loss.

If the congestion level is zero, then the congestion status is eliminated, and the MGC or CMS node resumes normal operations for the affected destination.

The MGC or CMS node treats a local congestion indication as a signaling point congestion indication to all destinations.

8.3.3.5 Congestion on the IP Network

If the MGC or CMS node detects congestion of the IP network to the SG, it reacts in the same manner as the SG. It uses a four level congestion scheme as defined in MTP level 3, and discards messages based on the priority of the messages as defined in the service information octet.

The method of detection and the measurement of congestion on the IP network is dependent on the lower layer used and on the implementation.

8.4 Message Format

The table below illustrates the format of an ISTP message.

Table 1. Message Format

Parameter Name	Size	Notes
MessageType	1 octet	Identifies the message type
MessageNature	1 octet	Identifies requests, responses or indications
MessageLength	2 octets	Length of the message to follow
ParameterId (1)	2 octets	The identifier of the parameter to follow
ParameterLength (1)	2 octets	The length of the parameter to follow
ParameterContent (1)	n octet(s)	The content of the parameter specified
ParameterId (n)	2 octets	The identifier of the parameter to follow
ParameterLength (n)	2 octets	The length of the parameter to follow
ParameterContent (n)	n octet(s)	The content of the parameter specified

8.4.1 Message Types

The following table lists the messages used in ISTP. The nature column indicates the nature of the event. *Req* is a request sent from the MGC or the CMS/CA to the SG, except for the Heartbeat message, which can be sent in either direction. *Rsp* is a response sent from the SG to the MGC or the CMS/CA, except for the Heartbeat message, which can be sent in either direction. *Ind* is an indication that is sent in either direction, or as defined in the notes column.

Table 2. Message Types

Message Type	ID	Nature	Notes
Circuit-Registration	0	Req, Rsp	
Circuit-De-Registration	1	Req, Rsp	
Circuit-Activation	2	Req, Rsp	
Exclusive-Circuit-Activation	3	Req, Rsp	
Circuit-Deactivation	4	Req, Rsp	
Forced-Circuit-Deactivation	5	Ind	Only sent by the SG
New-Work-Circuit-Activation	6	Req, Rsp	
New-Work-Circuit-Deactivation	7	Ind	Only sent by the SG
Subsystem- Registration	8	Req, Rsp	
Subsystem- De-Registration	9	Req, Rsp	
Subsystem- Activation	10	Req, Rsp	
Exclusive-Subsystem- Activation	11	Req, Rsp	
Subsystem- Deactivation	12	Req, Rsp	
Forced-Subsystem- Deactivation	13	Ind	Only sent by the SG
ISUP-Message-Transfer	14	Ind	Sent in both directions
TCAP-Message-Transfer	15	Ind	Sent in both directions
Signaling-Point-Inaccessible	16	Ind	Only sent by the SG
Signaling-Point-Accessible	17	Ind	Only sent by the SG
Subsystem-Inaccessible	18	Ind	Only sent by the SG
Subsystem-Accessible	19	Ind	Only sent by the SG
Signaling-Point-Congestion	20	Ind	Only sent by the SG
Local-Congestion	21	Ind	Only sent by the SG
SS7-Network-Accessible	22	Ind	Only sent by the SG
SS7-Network-Inaccessible	23	Ind	Only sent by the SG
Heartbeat	24	Req, Rsp	Sent in both directions
– reserved --	255	N/A	Reserved for future expansion

8.4.2 Message Nature

Table 3. Message Nature

Message Nature	ID	Notes
Request	0	
Response	1	
Indication	2	This is a unidirectional message
-- reserved --	255	Reserved for future expansion

8.4.3 Parameters

Parameters and their format are defined in this section. There are a few basic types, and a number of complex formats that follow in subsequent sections.

Table 4. Parameter Name References

Parameter Name	ID	Format	Reference
affectedPointCode	0	pointCode	section 8.4.3.11
calledPartyAddress	1	sccpPartyAddress	section 8.4.3.16
callingPartyAddress	2	sccpPartyAddress	section 8.4.3.16
cic	3	cic	section 8.4.3.2
circuitRange	4	circuitRange	section 8.4.3.3
cmsName	5	asciiString	section 8.4.3.1
congestionLevel	6	integer (1 octet)	section 8.5.4.6
destinationType	7	integer (1 octet)	section 8.4.3.4
inaccessibilityReason	8	integer (1 octet)	section 8.4.3.5
isupClientReturnValue	9	integer (1 octet)	section 8.4.3.7
isupTransferFormat	10	integer (1 octet)	section 8.4.3.8
mgcName	11	asciiString	section 8.4.3.1
normalizedISUPMsg	12	stream	section 8.4.3.9
normalizedTCAPMsg	13	stream	section 8.4.3.10
rawISUPMsg	14	stream	section 8.4.3.13
rawTCAPMsg	15	stream	section 8.4.3.14
routingLabel	16	routingLabel	section 8.4.3.15
ssn	17	integer (1 octet)	section 8.4.3.6
subsystem	18	subsystem	section 8.4.3.18
tcapClientReturnValue	19	integer (1 octet)	section 8.4.3.19
tcapTransferFormat	20	integer (1 octet)	section 8.4.3.20
transactionIdentifier	21	integer (4 octets)	section 8.4.3.6
– reserved –	65535	n/a	Reserved for future expansion.

8.4.3.1 asciiString

This generic parameter format is used for values containing textual information. It is a stream of octets containing printable ASCII characters. The string is NOT null terminated nor is it padded with spaces as imposed by some programming languages.

8.4.3.2 cic

Circuit identification codes as found in ISUP are stored in a two octet field, as found in the pertinent SS7 standards, and transmitted in the same order. Spare bits are set to zero.

8.4.3.3 CircuitRange

This parameter contains point codes and circuit identification that identify a range of circuits. It has a length of 10 octets total.

Table 5. CircuitRange

Field Name	Type	Size	Notes
gatewayPointCode	pointCode	3	The point code of this SSP, typically that of the gateway
adjacentPointCode	pointCode	3	The point code of the adjacent SSP
cicLowerBound	cic	2	The lower CIC value of the sieve, inclusive
cicUpperBound	cic	2	The upper CIC value of the sieve, inclusive

8.4.3.4 DestinationType

This parameter is encoded as a one-octet integer, and contains the type of the SS7 destination. It can have one of the following values:

Table 6. DestinationType

Value	Definition
0	network-cluster-member
1	network-cluster
2	network
3	all destinations

8.4.3.5 InaccesibilityReason

This parameter is encoded as a one-octet integer and contains the reason for the inaccessibility of the SS7 destination. It can have one of the following values:

Table 7. InaccesibilityReason

Value	Definition
0	remote network failure
1	network access failure
2	unknown destination

8.4.3.6 Integer

Integer values are stored as one, two or four octets representing a positive decimal value between 0 and 255 for single octet values, between 0 and 65535 for double octet values, and between 0 and 4,294,967,295 for four octet values. These values are transmitted in network order, with the high order octet transmitted first.

8.4.3.7 isupClientReturnValue

This parameter is encoded as a one-octet integer and contains the return code of an ISUP client request. It can have one of the following values:

Table 8. isupClientReturnValue

Value	Definition
0	successful and inactive
1	successful and active
2	duplicate entry

Value	Definition
3	unauthorized entry
4	invalid value
5	unsupported format
6	already active

8.4.3.8 isupTransferFormat

This parameter is encoded as a one-octet integer and contains the format to be used for exchange of ISUP messages. It can have one of the following values:

Table 9. isupTransferFormat

Value	Definition
0	raw ISUP messages
1	normalized ISUP messages

8.4.3.9 NormalizedISUPMsg

This parameter contains a normalized ISUP message, starting from the first octet of the CIC. A normalized ISUP message follows the encoding rules of the ANSI ISUP SS7 standards.

8.4.3.10 NormalizedTCAPMsg

This parameter contains a normalized TCAP message, starting from the first octet of the User Data parameter in SCCP. A normalized TCAP message follows the encoding rules of the ANSI SS7 TCAP standards. The parameters used within the component sections of the TCAP message follow the respective TCAP protocol standards of the messages being conveyed (i.e.: AIN, GSM, IS-41, LIDB, etc.).

8.4.3.11 pointCode

Point codes in ISTP are stored as a binary string of 3 octets in size. They use the same format as found in SS7 messages, with the first octet to be transmitted stored in the first octet of the parameter.

ANSI point codes occupy the full 3 octets, with the member in the first octet, the cluster in the second octet and the network in the third octet.

ITU point codes occupy the first octet and the lower 6 bits of the second octet, for a total of 14 bits out of a possible 24. The other bits are set to zero. They are also stored as defined in the respective standards, with the first octet to be transmitted stored in the first octet of the ISTP parameter.

8.4.3.12 QualityOfService

This parameter contains information on the quality of service requirements.

Table 10. QualityOfService

Field Name	Type	Size	Notes
sequenceControl	integer	1	0 – sequence guaranteed 1 – sequence not guaranteed
returnOption	integer	1	0 – return on error 1 – discard on error
priority	integer	1	0, 1 or 2. Not used in ITU, and should be set to zero

8.4.3.13 rawISUPMsg

This parameter contains a raw ISUP message, starting from the first octet of the CIC. A raw ISUP message follows the encoding rules of the local SS7 ISUP standards.

8.4.3.14 rawTCAPMsg

This parameter contains a normalized TCAP message, starting from the first octet of the User Data parameter in SCCP. A raw TCAP message follows the encoding rules of the local SS7 TCAP standards.

8.4.3.15 routingLabel

This parameter contains the information found in the MTP L3 routing label.

Table 11. routingLabel

Field Name	Type	Size	Notes
sio	integer	1	The service information octet
dpc	pointCode	3	The destination point code
opc	pointCode	3	The origination point code
sls	integer	1	The signaling link selection field

8.4.3.16 sccpPartyAddress

The SCCP party address contains the information found at the SCCP level for proper routing of the TCAP message to the destination. It has the following format.

Table 12. sccpPartyAddress

Field Name	Type	Size	Notes
addressIndicator	integer	1	The address indicator format can be found below
ssn	integer	1	The subsystem number
destinationPointCode	pointCode	3	The point code of the destination
globalTitleLength	integer	1	The length of the global title info to follow
globalTitle	stream	n	The global title information

The address indicator octet is further broken down into the following sub-fields:

Bit 8: Network Indicator, 0 – international and 1 – national

Bit 7: Routing Indicator, 0 – route on GTT, 1 – route on DPC/SSN

Bits 6-3: Global Title Type, as found in the SS7 message.

Bit 2: PC Present when set to 1.

Bit 1: SSN Present when set to 1.

Note that bits 1 and 2 have different definitions in ANSI and ITU. The ANSI rules are used for ISTP.

The format of the global title type (bits 6-3 of the address indicator) and of the global title field are a reflection of the local SS7 implementations.

8.4.3.17 stream

Native SS7 parameters and messages are stored in a stream of unsigned octets, and are transmitted in the same order as defined in the respective SS7 standards. The encoding of the parameters using this format is also specified in the respective SS7 standards.

8.4.3.18 subsystem

This parameter contains point code and the subsystem number that identify the CMS/CA application.

Table 13. subsystem

Field Name	Type	Size	Notes
localPointCode	pointCode	3	The point code of the CMS/CA
ssn	integer	1	The subsystem number

8.4.3.19 tcapClientReturnValue

This parameter is encoded as a one-octet integer and contains the return code of an TCAP client request. It can have one of the following values:

Table 14. tcapClientReturnValue

Value	Definition
0	successful and inactive
1	successful and active
2	duplicate entry
3	unauthorized entry
4	invalid value
5	unsupported format
6	already active

8.4.3.20 tcapTransferFormat

This parameter contains the format to be used for exchange of TCAP messages, and can have one of the following values:

Table 15. tcapTransferFormat

Value	Definition
0	raw TCAP messages
1	normalized TCAP messages

8.5 Messages

This section specifies the format of ISTP messages, and the presence of parameters within these messages. A mandatory parameter is indicated with the letter "M", whereas a conditional parameter is indicated with the letter "C". The columns "REQ", "RSP" and "IND" are request, response and indication, and correspond to the table in section 8.4.1. The encoding of the parameters is found in the previous sections.

There is no set order in which the parameters are stored in the message. An ISTP node must be prepared to receive the parameters in any order.

8.5.1 Circuit Registration and Activation Messages

This message set allows the MGC to request delivery of MSUs to the proper MGC node by the SG, and ensures correct mapping of IPCablecom resources to SS7 naming and addressing. The messages exchanged between the MGC and the SG are:

8.5.1.1 Circuit Registration

The MGC sends the SG a circuit registration request to reserve the specified circuit range with the requested transfer format. The SG responds to this message to confirm or reject the requested circuit range.

The circuit registration messages contain the following information:

Table 16. Circuit Registration

Parameter Name	REQ	RSP	Notes
mgcName	M	M	The name of the MGC element
circuitRange	M	M	The range of circuits to register
isupTransferFormat	M	M	Enumeration identifying the preferred format of the IP-bound ISUP messages
isupClientReturnValue	n/a	M	The return code for the operation

8.5.1.2 Circuit De-Registration

The MGC sends the SG a circuit de-registration request to indicate that it no longer wishes to reserve the specified circuit range for its use. The SG responds to this message, with the proper information in the IsupClientReturnValue parameter.

Table 17. Circuit De-Registration Requests

Parameter Name	REQ	RSP	Notes
mgcName	M	M	The name of the MGC element
circuitRange	M	M	The range of circuits to de-register
isupClientReturnValue	n/a	M	The return code for the operation

8.5.1.3 Circuit Activation

The MGC sends the SG a circuit activation request to indicate that the specified entry should be activated. The SG responds to this message to confirm or reject the activation request.

The circuit activation message contains the following information:

Table 18. Circuit Activation Requests

Parameter Name	REQ	RSP	Notes
mgcName	M	M	The name of the MGC
circuitRange	M	M	The range of circuits to activate
isupClientReturnValue	n/a	M	The return code for the operation

8.5.1.4 Forced Exclusive Circuit Activation

The MGC sends the SG a forced exclusive circuit activation request to indicate that the specified entry should be activated for exclusive use, regardless of the currently active MGC nodes. The SG responds to this message to confirm or reject the activation request.

The forced exclusive circuit activation message has the same format as the circuit activation message.

8.5.1.5 New Work Circuit Activation

The MGC sends the SG a new work circuit activation request to indicate that the specified entry should be activated for new work only. The SG responds this message to confirm or reject the activation request.

The new work circuit activation message has the same format as the circuit activation message.

8.5.1.6 Circuit Deactivation

The MGC sends the SG a circuit deactivation request to indicate that the specified entry be deactivated. The SG MUST respond to confirm or reject the deactivation request.

The circuit deactivation message has the same format as the circuit activation message.

8.5.1.7 Forced Circuit Deactivation

The SG sends a forced circuit deactivation indication to the MGC node to notify that it has been deactivated by another MGC node or other administrative function.

The forced circuit deactivation message has the following format:

Table 19. Forced Circuit Deactivation Indication

Parameter Name	IND	Notes
mgcName	M	The name of the MGC element
circuitRange	M	The range of circuits to register

8.5.1.8 New Work Circuit Deactivation

The SG sends a new work circuit deactivation indication to the MGC node to notify that it has been deactivated by another MGC node or other administrative function, for all new work on the circuit(s). The MGC node is still responsible for work already in progress.

The new work circuit deactivation message has the same format as the forced circuit deactivation message.

8.5.2 Subsystem Transaction Registration and Activation Messages

This message set allows the CMS to request delivery of MSUs to the proper MGC node by the SG, and ensures correct mapping of IPCablecom resources to SS7 naming and addressing. The messages exchanged between the CMS and the SG are:

8.5.2.1 Subsystem Registration

The CMS/CA sends the SG a subsystem registration request to reserve the specified subsystem with the requested transfer format. The SG MUST respond to this message to confirm or reject the requested subsystem.

The subsystem registration messages contain the following information:

Table 20. Subsystem Registration Requests

Parameter Name	REQ	RSP	Notes
cmsName	M	M	The name of the CMS/CA element
subsystem	M	M	The subsystem to register
tcapTransferFormat	M	M	Enumeration identifying the preferred format of the IP-bound TCAP messages
tcapClientReturnValue	n/a	M	The return code for the operation

8.5.2.2 Subsystem De-Registration

The CMS/CA sends the SG a subsystem de-registration request to indicate that it no longer wishes to reserve the subsystem for its use. The SG MUST respond to this message, with the proper information in the TcapClientReturnValue parameter.

Table 21. Subsystem De-Registration Requests

Parameter Name	REQ	RSP	Notes
cmsName	M	M	The name of the CMS/CA element
subsystem	M	M	The subsystem to de-register
tcapClientReturnValue	n/a	M	The return code for the operation

8.5.2.3 Subsystem Activation

The CMS/CA sends the SG a subsystem activation request to indicate that the specified entry should be activated. The SG MUST respond to this message to confirm or reject the activation request.

The subsystem transaction activation message contains the following information:

Table 22. Subsystem Activation Requests

Parameter Name	REQ	RSP	Notes
cmsName	M	M	The name of the CMS/CA element
subsystem	M	M	The subsystem to register
tcapClientReturnValue	n/a	M	The return code for the operation

8.5.2.4 Exclusive Subsystem Activation

The CMS/CA sends the SG an exclusive subsystem activation request to indicate that the specified entry should be activated, regardless of the current activate subsystems. The SG MUST respond to this message to confirm or reject the activation request.

The exclusive subsystem activation message has the same format as the subsystem activation message.

8.5.2.5 Subsystem Deactivation

The CMS/CA sends the SG a subsystem deactivation request to indicate that the specified entry be deactivated. The SG MUST respond to confirm or reject the deactivation request.

The circuit deactivation message has the same format as the subsystem transaction activation message.

8.5.2.6 Forced Subsystem Deactivation

The SG sends a forced subsystem deactivation indication to the CMS to notify that it has been deactivated by another CMS node or other administrative function.

The forced subsystem transaction deactivation message has the following format.

Table 23. Forced Subsystem Deactivation Indication

Parameter Name	REQ	Notes
cmsName	M	The name of the CMS/CA element
subsystem	M	The subsystem that has been deactivated

8.5.3 Message Transfer

SS7 message signaling units are exchanged between the MGC or the CMS/CA and SG using the following message.

8.5.3.1 ISUP-Message-Transfer

The MGC and the SG exchange ISUP messages using this message. Only one of the ISUP representation is found in the message (raw or normalized), depending on the *isupTransferFormat* parameter in the original registration request.

Table 24. ISUP-Message-Transfer

Parameter Name	IND	Notes
routingLabel	M	The normalized MTP L3 routing label
cic	M	The circuit identification code
normalizedISUPMsg	C	The normalized ISUP message to transfer, excluding the CIC.
rawISUPMsg	C	The raw (original) ISUP message to transfer, excluding the CIC.

8.5.3.2 TCAP-Message-Transfer

The CMS and the SG exchange TCAP messages using this message. Only one of the TCAP representation is found in the message (raw or normalized), depending on the *tcapTransferFormat* parameter in the original registration request.

When a TCAP message is sent from the CMS/CA to the SG, the transaction identifier found in the normalizedTCAPMsg or the rawTCAPMsg parameter gets overwritten by the SG before the message is sent on the SS7 links. Messages in the opposite direction do not get modified, although the ISTP transaction id mapped from the original or responding transaction id of the TCAP transaction id.

Table 25. TCAP-Message-Transfer

Parameter Name	IND	Notes
routingLabel	M	The normalized MTP L3 routing label
calledPartyAddress	M	The terminating party's address of the SCCP message
callingPartyAddress	M	The initiating party's address of the SCCP message
qualityOfService	M	The quality of service requirements
transactionIdentifier	M	The ISTP transaction identifier
normalizedTCAPMsg	C	The normalized TCAP message to transfer, excluding the CIC
rawTCAPMsg	C	The raw (original) TCAP message to transfer, excluding the CIC

8.5.4 Flow Control

Flow control messages and procedures are used to indicate to the MGC or the CMS the inability or difficulty for the SG to communicate with SS7 signaling points of interest. Most of these messages are a replication of the MTP primitives used between L4 applications and MTP L3.

There are no flow control messages and procedures initiated by the MGC, since the SG has no means of forwarding partial SSP congestion information at the MTP L3 level. If congestion is experienced between the MGC or the CMS and the SG, from the SG perspective, there are no procedures that are required.

8.5.4.1 Heartbeat

All ISTP nodes are expected to request and to respond to heartbeat messages. Heartbeat request are send on a periodic basis. The receiving end needs to promptly respond to the heartbeat request.

The heartbeat message contains no parameters.

8.5.4.2 Signaling Point Inaccessible

The SG sends the MGC or the CMS a signaling point inaccessible indication to notify that it cannot route SS7 traffic to the specified destination(s). The SG will send this message when:

- It detects that the destination is no longer accessible, either because of SS7 link failure or because it received a TFP.
- It receives a Message-Transfer from an MGC or a CMS with a point code for which it has no defined routeset (the SG will not send the indication more than once every second if the MGC or CMS does not stop its transfers to a specific point code).
- It receives a Message-Transfer from an MGC or a CMS for an inaccessible destination (the SG will not send the indication more than once every second if the MGC or CMS does not stop its transfers to a specific point code).
- A MGC successfully registers for circuits to a new point code, and that destination is inaccessible.
- A CMS successfully registers for subsystems to a new point code, and that destination is inaccessible.
- The SG will only send a signaling point inaccessible message to MGC and CMS nodes that are registered to communicate with the affected destination (using the adjacent point code field).

The message format of this message is:

Table 26. Signaling Point Inaccessible

Parameter Name	IND	Notes
routingLabel	M	The normalized MTP L3 routing label
destinationType	M	Type of the SS7 destination
inaccesibilityReason	M	The reason for the inaccessibility

8.5.4.3 Signaling Point Accessible

The SG sends the MGC and the CMS a signaling point accessible indication to notify that it can now route SS7 traffic to the specified destination(s). The SG will send this message when:

- It detects that the destination has become accessible, either because of SS7 link restoration or because it received a TFA or a TCA.
- A MGC successfully registers for circuits to a new point code, and that destination is accessible.
- A CMS successfully registers for subsystems to a new point code, and that destination is accessible.
- The SG will only send a signaling point accessible message to MGC and CMS nodes that are registered to communicate with the affected destination (using the adjacent point code field).

The message format of this message is:

Table 27. Signaling Point Accessible

Parameter Name	IND	Notes
routingLabel	M	The normalized MTP L3 routing label
destinationType	M	Type of the SS7 destination

8.5.4.4 Subsystem Inaccessible

The SG sends the CMS a subsystem inaccessible indication to notify that it cannot route SS7 traffic to the specified subsystem destination(s). The SG will send this message when:

- It detects that a destination subsystem is no longer accessible, because it received a SSP management message.
- It receives a TCAP-Message-Transfer from an CMS with a point code and subsystem number which is not accessible (the SG will not send the indication more than once every second if the CMS does not stop its transfers to a specific subsystem).
- The SG will only send a subsystem inaccessible message to CMS nodes that are registered to communicate with the affected destination (using the adjacent point code field).

The message format of this message is:

Table 28. Subsystem Inaccessible

Parameter Name	IND	Notes
subsystem	M	The destination subsystem number
inaccesibilityReason	M	The reason for the inaccessibility

8.5.4.5 Subsystem Accessible

The SG sends the CMS a signaling point accessible indication to notify that it can now route SS7 traffic to the specified destination(s). The SG will send this message when it detects that the destination subsystem has become accessible, because it received an SSA or an SSP.

The SG will only send a subsystem accessible message to CMS nodes that are registered to communicate with the affected destination (using the adjacent point code field).

The message format of this message is:

Table 29. Subsystem Accessible

Parameter Name	IND	Notes
subsystem	M	The destination subsystem

8.5.4.6 Signaling Point Congestion

The SG sends a signaling point congestion message to indicate to the CMS that the SS7 network leading to the specified destination is congested, or that the congestion state has been lifted. The SG will send this message when it receives a TFC message from the adjacent STP.

The Destination-Congestion message contains the following information:

Table 30. Signaling Point Congestion

Parameter Name	IND	Notes
affectedPointCode	M	The affected point code
destinationType	M	Type of the SS7 destination
congestionLevel	M	The congestion level. The range is from 0 (none) to 3 (high)

8.5.4.7 Local Congestion

The SG sends a local congestion message to indicate to the MGC and the CMS that the SS7 links to the adjacent nodes are congested, or that the congestion state has been lifted. The SG will send this message when it detects local SS7 link congestion changes to its adjacent nodes.

The local congestion message contains the following information:

Table 31. Local Congestion

Parameter Name	IND	Notes
congestionLevel	M	The congestion level. The range is from 0 (none) to 3 (high)

8.5.4.8 SS7 Network Accessible

The SG sends a SS7 network accessible message to indicate to the MGC and the CMS that it has regained access to the SS7 network because of the successful alignment of the local links and the termination of the MTP Restart procedure.

The SS7 network accessible message contains no parameters.

8.5.4.9 SS7 Network Inaccessible

The SG sends a SS7 network inaccessible message to indicate to the MGC and the CMS that it has lost access to the SS7 network because of the failure of all local links.

The SS7 network inaccessible message contains no parameters.

Appendix I SCTP and TCP Usage Recommendations

SCTP is the preferred transport mechanism for ISTP. However, TCP can also be used. Usage recommendations for both of these protocols are described in this appendix.

I.1 SCTP Usage Recommendations

SCTP will provide the preferred transport mechanism for ISTP. There are a number of considerations regarding the use of SCTP in a near real-time context for the transportation of ITSP. This section examines a few concerns and proposes some potential solutions that can provide a higher quality of service.

The design of the network should support the desired degree of reliability and real time performance. This can mean providing fully redundant DS-0 paths dedicated to signaling traffic only. Sharing IP connection with other traffic over the signaling links can result in performance and reliability degradation, and should only be considered in networks where availability, reliability, communication completion, and quality requirements can be relaxed.

I.1.1 SCTP Stream Mapping

SCTP streams provide a means to avoid the head of line blocking issue that exists within TCP. The use of SCTP streams by ISTP is recommended in order to minimize transmission and buffering delays, therefore improving the overall performance and reliability of the signaling elements. The distribution of the MTP3 user messages over the various streams should be done in such a way to minimize message mis-sequencing, as required by the SS7 User Parts.

The ISTP at both the SG and MGC should support the assignment of signaling traffic into streams within an SCTP association. Traffic that requires sequencing must be assigned to the same stream. To accomplish this, MTP3-User traffic should be assigned to individual streams based on the SLS value in the MTP3 Routing Label.

I.1.2 SCTP Congestion Information

Implementations of SCTP can provide local and IP network congestion information to its upper layer. If this congestion information is available, it should be used by ISTP. The ISTP layer will be informed of IP network congestion by means of an implementation-dependent function (e.g., an implementation-dependent indication from the SCTP of IP network congestion).

When a SG determines that the transport of SS7 messages to a Signaling Point is encountering congestion, the SG should trigger SS7 MTP3 Transfer Controlled management messages to originating SS7 nodes. The triggering of SS7 MTP3 Management messages from a SG is an implementation-dependent function.

At a MGC, the SCTP congestion is indicated to local MTP3-Users by means of an MTP-Status primitive indicating congestion, to invoke appropriate upper layer responses, as per current MTP3 procedures.

I.2 TCP Usage Recommendations

TCP can be used in early phases of IPCablecom as a transport mechanism until an agreed upon standard is defined. However, there are a number of considerations regarding the use of TCP in a near real-time context for the transportation of ITSP. This section examines a few concerns and proposes some potential solutions that can provide a higher quality of service.

The design of the network should support the desired degree of reliability and real time performance. This can mean providing fully redundant DS-0 paths dedicated to signaling traffic only. Sharing IP connection with other traffic over the signaling links can result in performance and reliability degradation, and should only be considered in networks where availability, reliability, communication completion, and quality requirements can be relaxed.

I.2.1 Delaying of Packets

TCP was originally designed for supporting multiple user sessions over a slow network. In order to optimize network utilization, the Nagle algorithm was introduced for keyboard input users. Essentially, this algorithm delays the transmission of a packet until a sufficiently large transmit buffer is accumulated or until a certain period of time (usually around 200 milliseconds) elapses.

Due to the real-time nature of SS7 traffic, it is advisable to disable the Nagle algorithm for socket communication with the Signaling Gateway. Not disabling this feature would introduce unnecessary delay in the flow of SS7 messages. On most Unix based platforms, the Nagle algorithm can be disable by issuing the following system call on the socket's file descriptor:

Example 1: Setting the TCP_NODELAY Option

```
/* set the TCP No-delay flag (disable Nagle algorithm) */
int flag = 1;
setsockopt(fd, IPPROTO_TCP, TCP_NODELAY, &flag,sizeof(flag));
```

Most other languages and platforms have a similar feature to disable the Nagle algorithm, usually known as the TCP_NODELAY option.

I.2.2 Non-Blocking Interface

By default, most operating systems provide a blocking interface for TCP/IP sockets. Although it can allow for an improved error recovery scheme, it has an impact on the performance of the communication channel.

Essentially, a system call such as send() with blocking interface never returns until the operating system confirms that the message was successfully stored in the transmit buffer.

It can be desirable for user parts of the Signaling Gateway to use a non-blocking interface in order to improve performance and to support asynchronous events using the select() function call on a UNIX based architecture. A non-blocking socket interface can be setup by using the following call on the newly created socket.

Example 2: Setting the O_NONBLOCK Option

```
/* set the socket to non blocking */
fcntl( fd, F_SETFL, O_NONBLOCK );
```

Most other languages and platform have a similar feature.

I.2.3 Disable TCP Socket Linger

When TCP sockets are closed, they pass through a TIME_WAIT state. This state can keep the socket open for several minutes. This can be problematic for some applications.

The TIME_WAIT state can be bypassed by setting the linger time on the socket to zero. On most Unix based platforms, the linger time can be set to zero by issuing the following system call on the socket's file descriptor:

Example 3: Setting the SO_LINGER time Option

```
sockLinger.l_onoff = 1;
sockLinger.l_linger = 0;
setsockopt( fd, SOL_SOCKET, SO_LINGER,
(char*)&sockLinger, sizeof(sockLinger) );
```

Appendix II ISTP Message Flows and Timer Definitions

II.1 Timers

This section defines the timers used by the MGC and SG to monitor the responses of ISTP messages. This specification does not mandate the action to take when a timer expires. All timers should be user configurable.

Table 32. ISTP Message Response Timers

Timer ID	Default Time-out	Range	Purpose	Started when the following messages are sent	Stopped when
Session-timer	30 seconds	1 – 120 seconds	Monitor session-based messages	Circuit-Registration Circuit-De-Registration Circuit-Activation Circuit-Deactivation Exclusive-Circuit-Activation Forced-Circuit-Deactivation New-Work-Circuit-Activation New-Work-Circuit-Deactivation	Corresponding ACK or NACK messages are received
Transaction-timer	4 seconds	1 – 30 seconds	Monitor transaction-based messages	ISUP- Message-Transfer TCAP- Message-Transfer	Corresponding ACK or NACK messages are received
Heartbeat-timer	1 second	10 ms –60 seconds	Monitor heartbeat request	Heartbeat request	Heartbeat response is received

It is the responsibility of the message transmitting entity to provide suitable time outs for all outstanding commands, and to retry commands when time outs have been exceeded. Furthermore, when repeated commands fail to be acknowledged, it is the responsibility of the transmitting entity to seek redundant services and/or clear existing or pending connections. Suitable alarms should also be raised in accordance with standard error practices.

II.2 MGC Requests ISUP/TUP Service Procedure

This scenario describes the registration and activation process when an MGC requests ISUP/TUP services from a SG.

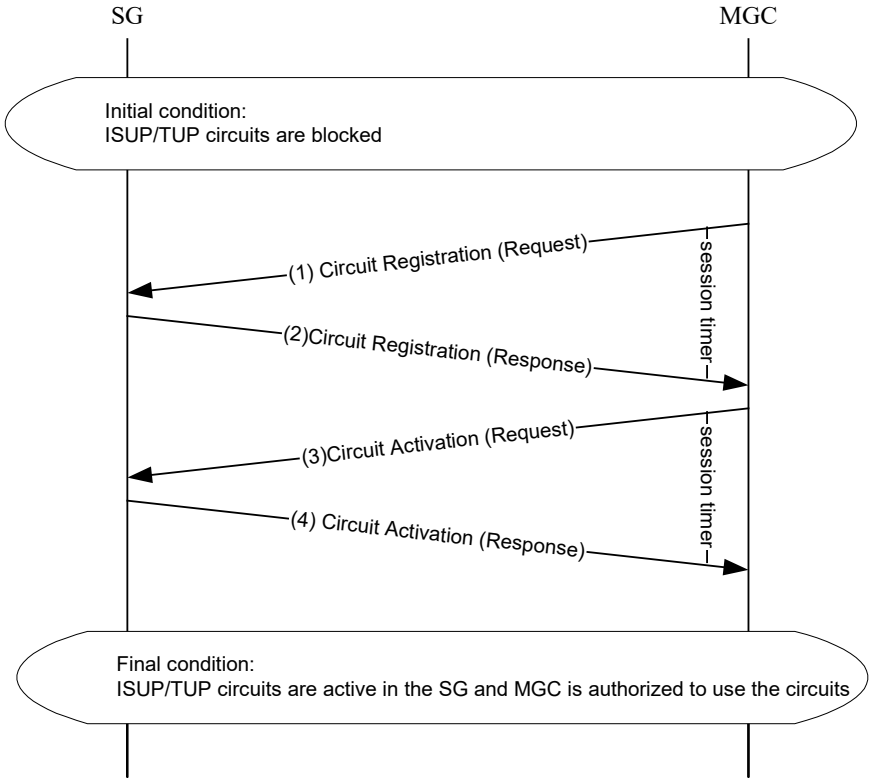

Figure 7. MGC Requests ISUP/TUP Service

- MGC sends a Circuit Registration request to the SG to reserve a group of circuits for its use. The session timer is started to monitor the response from SG. The request specifies the IP address of MGC, the circuit range, and ISUP message format, raw or normalized ISUP messages. Note that the local point code field in the circuitRange parameter will be blank in the request since MGC does not own any point code.
- The SG returns a Circuit Registration response to grant the reservation request on the specified circuits to the MGC. In the response, SG should fill in the local point code field in the circuitRange parameter with its point code and isupClientReturnValue parameter with proper return value. Upon receiving this message, MGC cancels the session timer. If the timer expires before receiving a response from SG, MGC shall take proper action.
- If the return code in the Circuit Registration response is *successful_and_inactive* and MGC is ready to service the ISUP/TUP messages on the circuits, it sends a Circuit Activation request to SG to activate the circuits. The session timer is started to monitor the response from SG.
- The SG sends a Circuit Activation response to the MGC. If the isupClientReturnValue field is set to *successful_and_active*, the MGC is granted the right to use the specified circuits. Upon receiving this message, MGC cancels the session timer. If the timer expires before receiving a response from SG, MGC shall take proper action.

II.3 MGC Terminates ISUP/TUP Service Procedure

This scenario describes the de-registration and de-activation process as an MGC terminates the ISUP/TUP service from a SG.

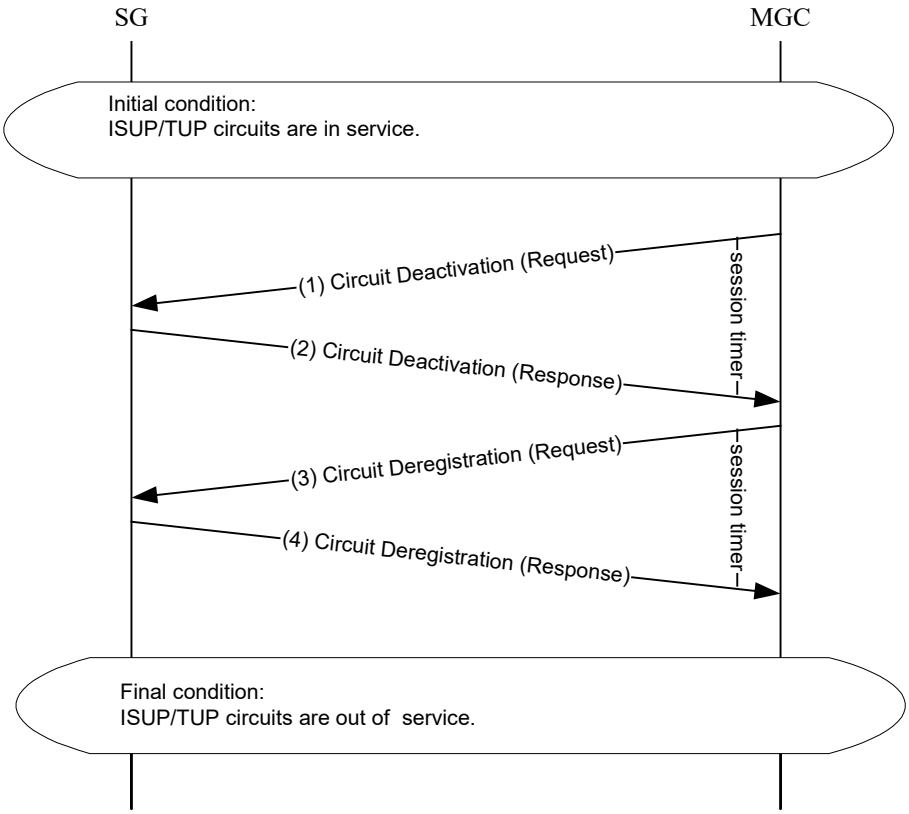

Figure 8. MGC Terminates ISUP/TUP Service

- MGC sends a Circuit Deactivation request to SG to deactivate the specified circuits. Once a circuit is deactivated, SG shall discard any ISUP/TUP messages associated with the deactivated circuits. The session timer is started to monitor the response from SG.
- SG sends a Circuit Deactivation response to acknowledge that the requested circuits are deactivated. If the deactivation is successful, the isupClientReturnValue should be set to *successful_and_inactive*. Upon receiving this message, MGC cancels the session timer. If the timer expires before receiving a response from SG, MGC shall take proper action.
- MGC sends a Circuit Deregistration request to the SG to free up the specified circuits. The session timer is started to monitor the response from SG.
- SG sends a Circuit Deregistration response to acknowledge the de-registration. If the deregistration is successful, the isupClientReturnValue should be set to *successful_and_inactive.* Upon receiving this message, MGC cancels the session timer. If the timer expires before receiving a response from SG, MGC shall take proper action.

II.4 Residential CA Requests TCAP Service Procedure

This scenario describes the registration and activation process when a residential CA requests the TCAP service from a SG.

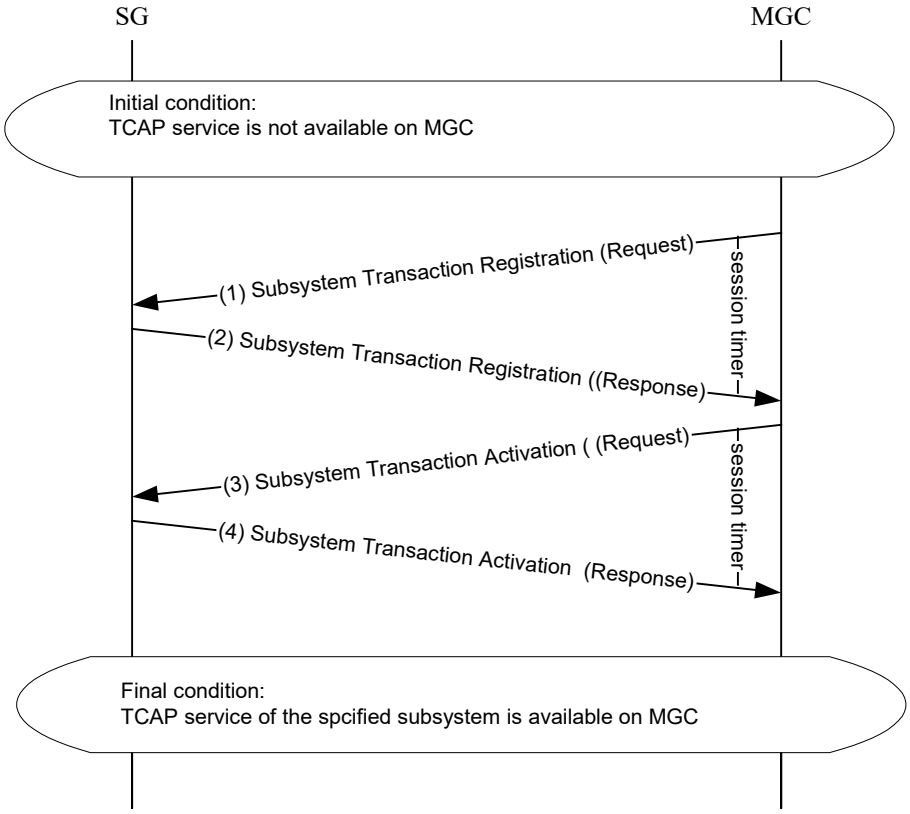

Figure 9. MGC Requests TCAP Service

- CA sends a Subsystem Transaction Registration request, including SSN, and SCCP service type, to the SG request TCAP service. The session timer is started to monitor the response from SG.
- SG returns a Subsystem Transaction Registration response to MGC. The tcapClientReturnValue parameter indicates if the registration is successful or not. Upon receiving the response, MGC cancels the session supervision timer. If the timer expires before receiving a response from SG, MGC shall take proper action.
- If the registration is successful, CA sends Subsystem Transaction Activation request to the SG to activate the TCAP service. The session timer is started to monitor the response from SG.
- SG returns a Subsystem Transaction Activation response to the CA. The tcapClientReturnValue parameter indicates if the registration is successful or not. Upon receiving the response, MGC cancels the session supervision timer. If the timer expires before receiving a response from SG, MGC shall take proper action.

II.5 Residential CA Terminates TCAP Service Procedure

This scenario describes the de-registration and de-activation process as a residential CA terminates the TCAP service from a SG.

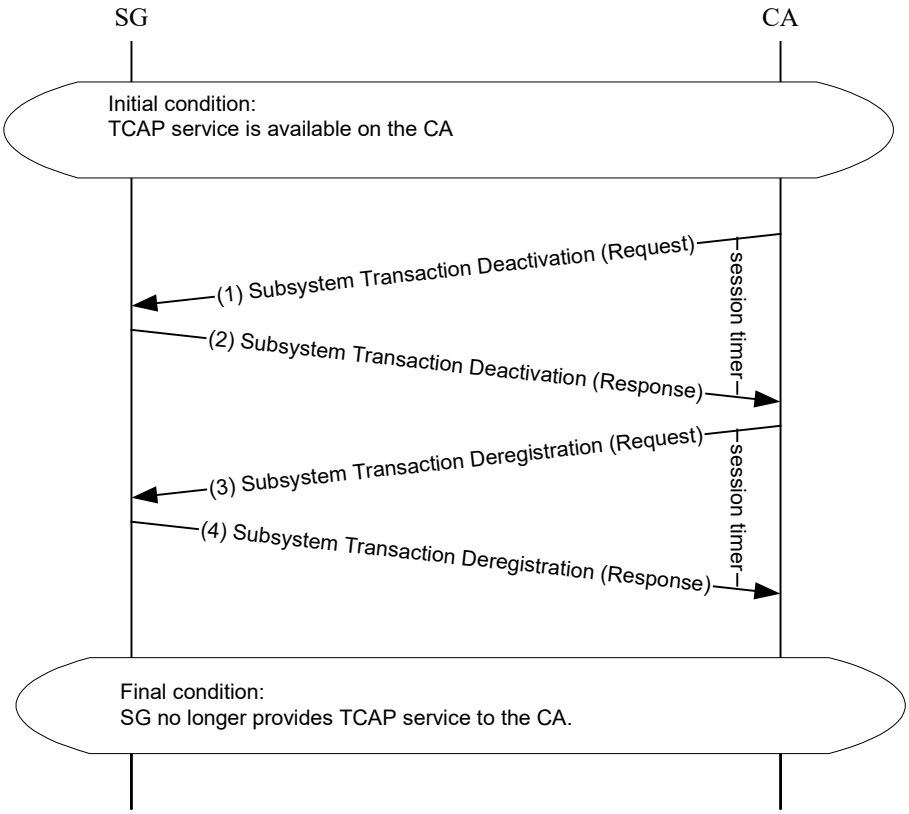

Figure 10. CA Terminates TCAP Service

- CA sends a Subsystem Transaction Deactivation request to SG to deactivate the TCAP service. A session timer is started on MGC to monitor the response from SG.
- SG returns a Subsystem Transaction Deactivation response with the tcapClientReturnValue parameter indicating if the deactivation is successful or not. MGC cancels the session timer upon receiving the response from SG. If the timer expires before receiving a response from SG, MGC shall take proper action.
- CA sends a Subsystem Transaction De-registration request to SG to deregister the TCAP service. A session timer is started on MGC to monitor the response from SG.
- SG returns a Subsystem Transaction De-registration response with the tcapClientReturnValue parameter indicating if the deactivation is successful or not. MGC cancels the session timer upon receiving the response from SG. If the timer expires before receiving a response from SG, MGC shall take proper action.

II.6 A Typical Origination Communication

This flow demonstrates a typical communication originated from a residential gateway and is extended to PSTN network over ISUP trunk. It is assumed that MGC has registered and activated ISUP service on SG.

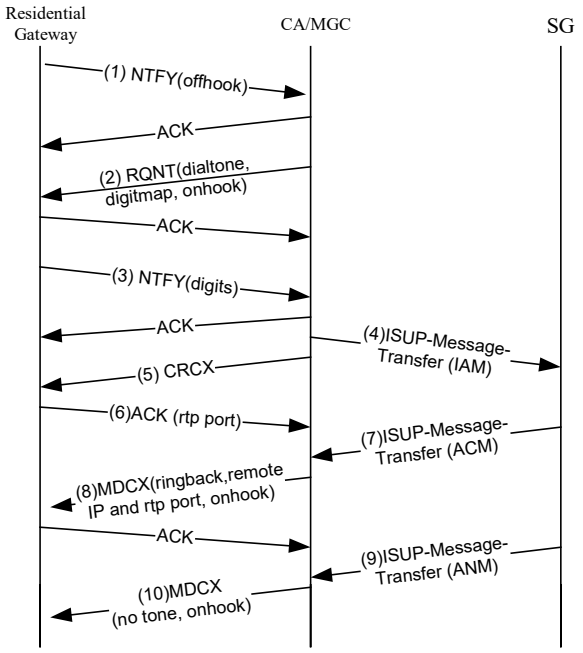

Figure 11. A Typical Origination Communication

- A subscriber activates the voice device connected to the RGW. The RGW detects the offhook and sends a notify event to the CA with observed event set to offhook.
- CA sends a notification request to RGW with digitmap, signal set to dial tone, and observe event set to onhook.
- RGW sends a notify message after digits are collected.
- CA analyzes the digits and determines to route the communication to the PSTN network over an ISUP trunk. CA establishes a communication to the MGC, which selects an ISUP trunk and initiates a communication by sending an ISUP-Message-Transfer (IAM) message to the SG.
- In the mean time, CA sends a create connection message to the RGW.
- RGW returns an ACK event with the RTP port number, which serves this communication.
- When the terminating party is alerted, the remote switch sends back the ACM message. SG then forwards the ACM in a ISUP-Message-Transfer message to MGC.
- MGC forwards the ACM message to CA, and CA sends a modification connection message to RGW instructing the RGW to apply back notification tone. The IP address and RTP port of the ISUP circuit on the MG are also sent down in this message.
- When the terminating party answers the communication, remote switch sends an ANM. SG sends the an ISUP-Message-Transfer (ANM) to MGC.
- MGC forwards the ANM to the CA, CA then sends a modification connection to RGW to turn off the back notification tone and set the mode to full duplex.

II.7 800 Number Service

This flow demonstrates the message flow of an 800 number service scenario. It is assumed that CA has registered and activated the 800 number service subsystem previously with the SG.

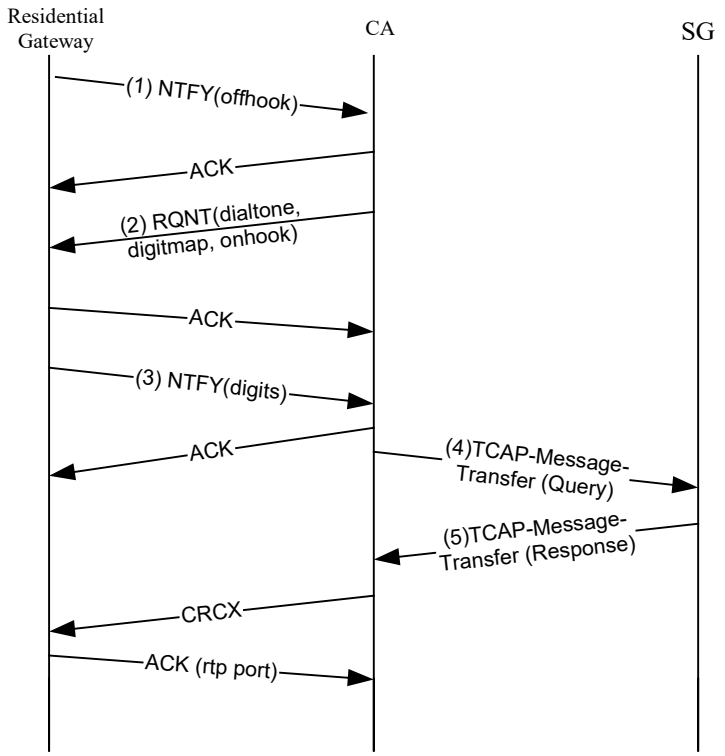

Figure 12. 800 Number Service

- The subscriber activates the voice device connected to the RGW. The RGW detects the offhook and sends a notify event to the CA with observed event set to offhook.
- CA sends a notification request to RGW with digitmap, signal set to dial tone, and observe event set to onhook.
- RGW sends a notify message after digits are collected.
- CA analyzes the incoming digits and detects that an 800 number is dialed. It sends a QUERY in the TCAP-Message-Transfer to the 800 database through SG. A supervision timer is stared by the CA. If the timer expires before SG returns a response, CA should provide proper intercept treatment to terminate the communication.
- SG returns a RESPONSE in the TCAP-Message-Transfer to the CA. CA then continues the communication setup.

II.8 MGC Failover Procedure

This flow demonstrates the failover procedure when the MGC runs in redundant mode.

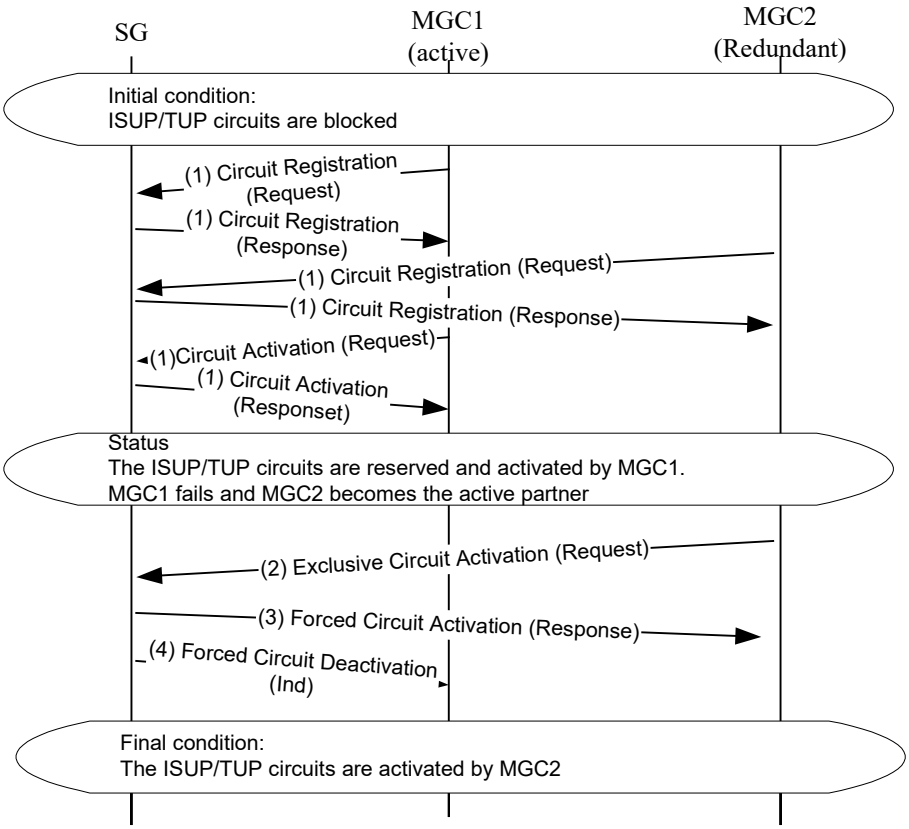

Figure 13. MGC Failover Procedure

- MGC1 and MGC2 are a redundant pair to serve the same set of ISUP/TUP circuits. Both MGC1 and MGC2 register to reserve the circuits and MGC1 activates the circuits.
- When MGC1 fails, MGC2 assumes its responsibilities. MGC2 sends an Exclusive Circuit Activation request to SG requesting to activate the specified circuits regardless of the status the circuits. A supervision timer is started to monitor the response from SG.
- SG returns an Exclusive Circuit Activation response to grant the request if the MGC2 has previously registered for the circuits. Upon receiving this message, MGC2 cancels the supervision timer. If the timer expires before receiving a response from SG, MGC2 shall take proper action.
- SG sends a Forced Circuit Deactivation indication to MGC1 indicating that the specified circuits have been activated by another MGC. No response is expected to this message.

II.9 MGC Switchover Procedure

This flow demonstrates the operator controlled switchover procedure when the MGC runs in redundant mode.

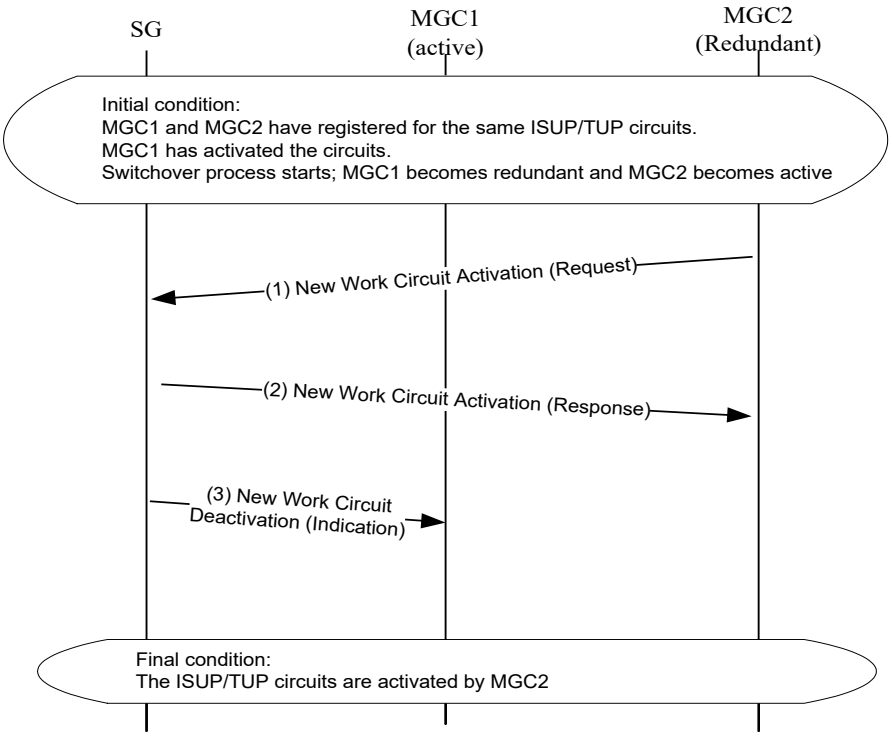

Figure 14. MGC Switchover Procedure

- MGC1 switches over to MGC2. MGC2 sends a New Work Circuit Activation request to SG. The session timer is started to monitor the response from SG.
- Upon receiving the New Work Circuit Activation request, SG returns a New Work Circuit Activation response to grant the request. From this point on, SG will route ISUP/TUP messages for the existing communications to MGC1 and ISUP/TUP messages for new communications to MGC2. Upon receiving the response, MGC2 cancels the session timer. If the timer expires before receiving a response from SG, MGC2 shall take proper action.
- SG sends a New Work Circuit Deactivation indication to MGC1 indicating that the specified circuits have been activated by another MGC.