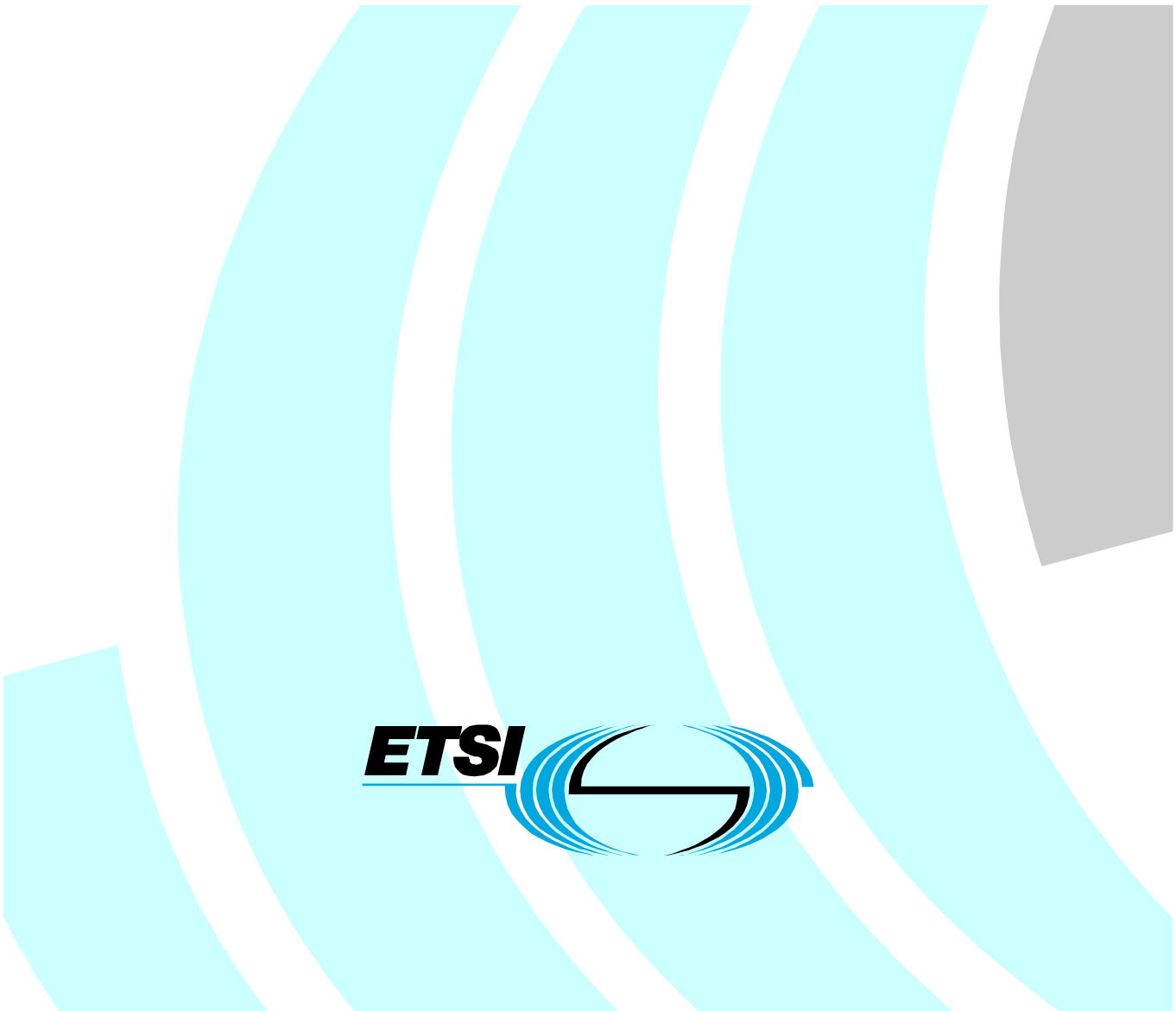
ETSI TS 101 909-12 V1.1.1 (2002-11)

Technical Specification

Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 12: Internet Signalling Transport Protocol (ISTP)



Reference
DTS/SPAN-130290

Keywords
IP, protocol, transport

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Services and Protocols for Advanced Networks (SPAN).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [3].

Introduction

This version is based on the 8TD112r2 from SPAN #78 in June 02 and the direct continuation of D8-36 presented at TC-AT-D in July 02. The main changes are due to the new mechnism for OTID assignment and the additions in the Subsystem registration. Proposed text changes from Ray Forbes are also covered.

1 Scope

The present document describes the Internet Signalling Transport Protocol (ISTP) to implement Signalling System No. 7 signalling interconnection to a distributed IPCablecom architecture.

The present document addresses the protocol to implement ETSI SS7 used for signalling interconnection in a distributed IPCablecom architecture. Specifically, it defines the messages and procedures for transporting SS7 ISUP, and TCAP messages as defined by ETSI specifications between the IPCablecom control functions (Media Gateway Controller and Call Management Server) and the SS7 Signalling Gateway. The IPCablecom Networks are always connected to the PSTN/ISDN using standard ETSI SS7 interfaces Ref (ISUP, MTP and SCCP)

Areas beyond the scope of the present document include:

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

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ETSI EN 300 356: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP) version 4 for the international interface".

[2] ETSI ETS 300 287-1 (Edition 2): "Integrated Services Digital Network (ISDN); Signalling System No.7; Transaction Capabilities (TC) version 2; Part 1: Protocol specification [ITU-T Recommendations Q.771 to Q.775 (1993), modified]".

[3] ETSI TS 101 909-1: "Digital Broadband Cable Access to the Public Telecommunications Network; IP Multimedia Time Critical Services; Part 1: General ".

3 Definitions, abbreviations and conventions

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Access Node (AN): As used in the present document, an Access Node is a layer two termination device that terminates the network end of the J.112 connection. It is technology specific. In ITU-T Recommendation J.112 annex A it is called the INA while in Annex B it is the CMTS.

Cable Modem (CM): layer two termination device that terminates the customer end of the J.112 connection

Gateway: devices bridging between the IPCablecom IP Voice Communication world and the PSTN

NOTE: Examples are the Media Gateway which provides the bearer circuit interfaces to the PSTN and transcodes the media stream, and the Signalling Gateway which sends and receives circuit switched network signalling to the edge of the IPCablecom network.

IPCablecom: ETSI project that includes an architecture and a series of Recommendations that enable the delivery of real time services over the cable television networks using cable modems

Signalling Gateway (SG): signalling agent that receives/sends SCN native signalling at the edge of the IP network

NOTE: In particular the SS7 SG function translates variants ISUP and TCAP in an SS7-Internet Gateway to a common version of ISUP and TCAP.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AN	Access Node
ANS	Announcement Server
ATM	Asynchronous Transfer Mode
CA	Call Agent
CIC	Circuit Identification Code
CID	Circuit ID
CM	Cable Modem
CMS	Call Management Server
DNS	Directory Name Server
DPC	Destination Point Code
HFC	Hybrid Fibre/Coaxial [cable]
IP	Internet Protocol
ISTP	Internet Signalling Transport Protocol
ISUP	ISDN User Part
LAN	Local Area Network
MAC	Media Access Control
MG	Media Gateway
MGC	Media Gateway Controller
MTA	Media Terminal Adapter
MTP	Message Transfer Part
NI	Network Identifier
OPC	Origination Point Code
OTID	Origination Transaction Identity
PHY	Physical Layer
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real Time Protocol
SCCP	Signalling Connection Control Part
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
SG	Signalling Gateway
SIP	Session Initiation Protocol
SLS	Signalling Link Selection
SS7	Signalling System No. 7
SSN	Switching Signalling Node
SSP	Signal Switching Point
TCAP	Transaction Capabilities Application Part
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WAN	Wide Area Network

3.3 Convention

If the present document is implemented, the key words "MUST" and "SHALL" are to be interpreted as indicating a mandatory aspect of the present document.

4 Signalling Protocols

The signalling protocols used for interconnection in a distributed IPCablecom PSTN gateway architecture shall be designed to support ETSI Signalling System No. 7 (SS7).

5 Void

6 Overview and background motivation

6.1 Service goals

Cable operators are interested in deploying high-speed data and multimedia communications services on cable television systems. It is necessary to have a series of interface Recommendations that will permit the early definition, design, development, and deployment of packetized data-based services over cable systems on a 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-fibre/coax (HFC) cable access network by utilizing ITU-T Recommendation J.112 as the basic foundation for data transport. This is shown in simplified form in figure 1.

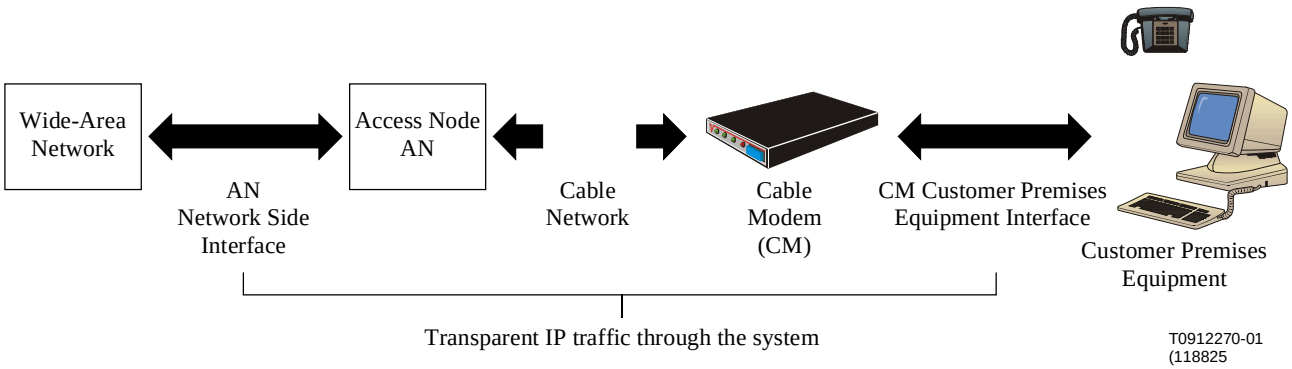


Figure 1: Transparent IP traffic through the data-over-cable system

The transmission path over the cable system is realized at the headend by an Access Node and at each customer location by a CM. The intent is for operators to transfer IP traffic transparently between these interfaces, thereby providing the basic transport mechanism for data-based multimedia services.

When providing voice and other multimedia services over the J.112 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 signalling;
- quality of service control;
- call control signalling 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. The present document, the IPCablecom Internet Signalling Transport Protocol (ISTP) addresses the issue of call control signalling interoperability with the existing public network.

6.2 IPCablecom reference architecture

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

Subscriber equipment consists of a Media Terminal Adapter (MTA), the primary purpose 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 that connects via a local area network (LAN) interface (e.g. IEEE 802.3) to a CM. The second is an embedded MTA, which integrates the standalone MTA functions with the 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 fibre-coax (HFC) J.112 enabled cable access network with J.112 Quality of Service (QoS). The J.112 HFC access network terminates at the head end Access Node. The Access Node provides either a bridging point or a routing point to the backbone managed IP network.

The Call Management Server (CMS) provides control, routing, and signalling 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 local 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 transit switch functionality as well as local. A SIP-proxy may also be contained within a CMS, although IPCablecom does not 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 signalling information related to the communication to the PSTN through the services of the Signalling Gateway (SG). This signalling 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 (freephone 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 signalling and convert it to signalling 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.

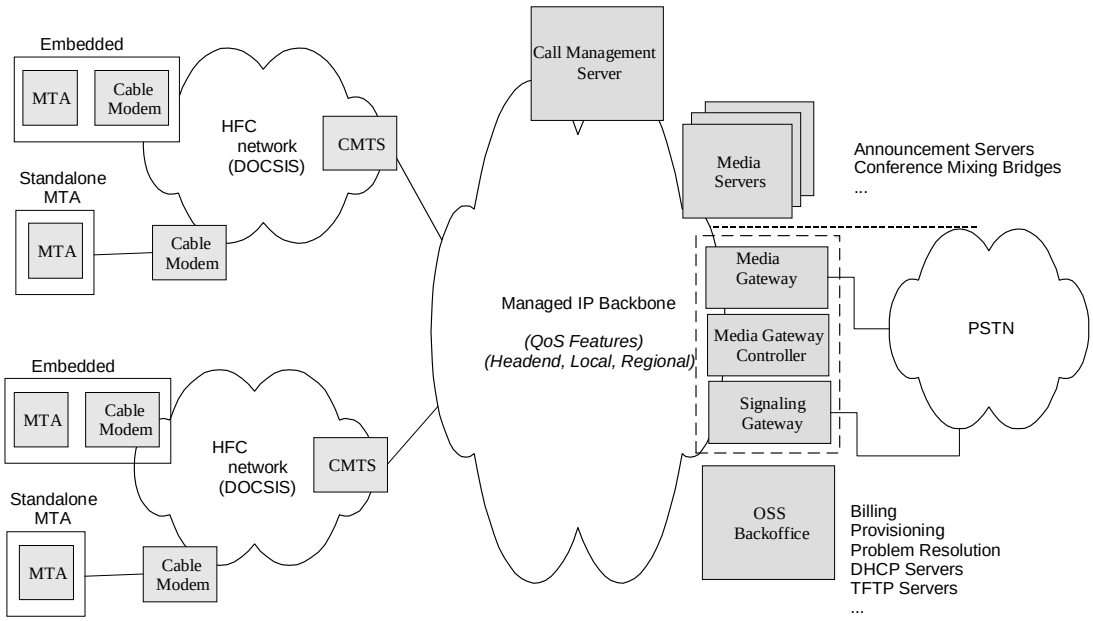


Figure 2: IPCablecom reference architecture

6.3 Introduction to ISTP

ISTP contains features for initialization; address mapping from the SS7 domain to the IP domain; message delivery for SS7 Integrated Services Digital Networks (ISDN) User Part (ISUP), Transaction Capabilities Application Part (TCAP); congestion management; fault management; maintenance operations; and redundant configuration support. ISTP bridges the gap between basic IP transport mechanisms and application level signalling. Although not a translation of the SS7 Message Transport Protocol 3 (MTP3) and Signalling 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 distributes transparently the ISUP and TCAP functions into multiple elements while retaining the computational intensive SCCP/MTP2/MTP3 SS7 stack elements in the Signalling Gateway (see figure 3). This also keeps the SCCP Global Title tables in a secure central location, as preferred by SS7 network operators. This breakdown also allows ISTP-User applications to have access to all the 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 signalling 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.

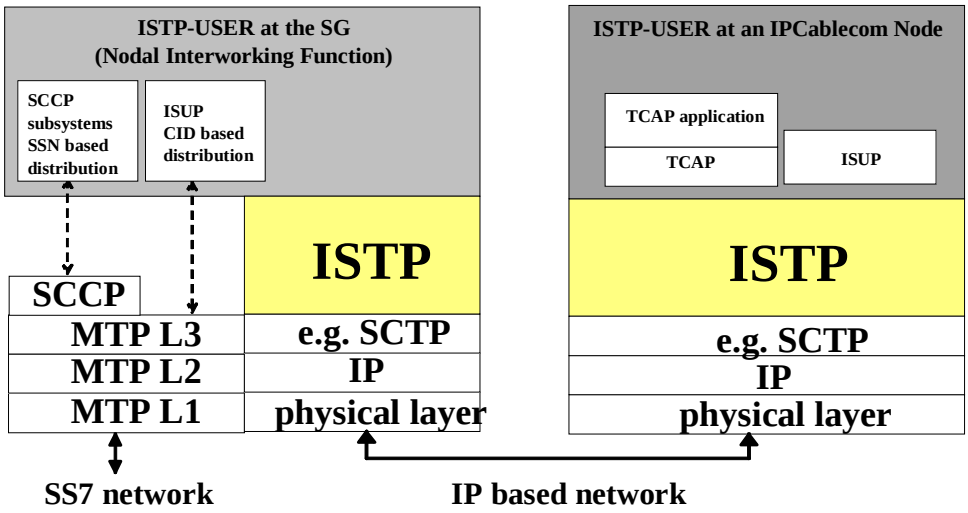


Figure 3: Protocol stack in IPCablecom elements

The ISTP is designed to support a wide variety of configurations, ranging from a non-redundant SS7 Signalling Gateway serving a single non-redundant Media Gateway Controller to a distributed, fully redundant SS7 Signalling 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 signalling communications. For the first phase of IPCablecom this includes 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 Origination Transaction ID (OTID) from the SS7 side of the SG to the transaction ID used on the IPCablecom side and vice versa.
- ISUP/TCAP Message Delivery Using Reliable Transport.
- Maintenance Operations.
- Activation/Deactivation of Circuit IDs within the SS7 Gateway. (The actual physical circuits terminate on the Media Gateway.)
- Error Recovery Due To Faults.
- SS7 Signalling Point Inaccessible.
- SS7 Signalling Network Inaccessible.
- MGC Inaccessible.
- CMS Inaccessible.
- Error Recovery Due To Congestion.
- Signalling Point Congested.
- Signalling Link Congested.

- MGC Congested.
- CMS Congested.

The above functions are implemented messages and procedures defined in the present document.

In order to meet the performance and reliability requirements mandated by IPCablecom and SS7 interconnection, ISTP requires the services of an underlying reliable transport service. The reliable transport preferred is Stream Control Transport Protocol (SCTP) as defined in the IETF SIGTRAN working group in RFC 2960 and RFC 3309. 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.

6.4 Specification goals

The goal of the present document is to meet and satisfy the business and technical requirements of cable operators, including the following:

- Support for cable companies' penetration into residential and business markets for multimedia 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 multimedia) 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/E1 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 simplified network (simplex connections) to support lower cost enterprise and customer premise implementations.

6.5 Specification interfaces

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

- *SS7 Signalling Gateway to Media Gateway Controller*: Enables signalling interconnection between the SS7 network and the Media Gateway Controller for SS7 ISUP message interworking. ISUP is used for out-of-band call signalling in the PSTN.
- *SS7 Signalling Gateway To TCAP User*: Enables signalling 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 freephone calling and number portability (NP) routing.

7 Architecture

7.1 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). At this time, only the Call Management Server, the Media Gateway controller, and the Signalling 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 signalling, 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 signalling over IP packets.
- The second is the switched circuit network for transport of voice, fax, and modem data.
- The third is the SS7 signalling based network for reliable transport of critical signalling information. The SS7 signalling network signalling is used to control the switched circuit network.

The SS7 signalling 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 signalling information is exchanged with the PSTN via the signalling 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 trunks. The Signalling 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 signalling 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 signalling will still be required to ensure cross network interoperability; this will be true whether the SS7 signalling runs over SCCP/MTP3/2/1 or over ATM or other protocol. In such a case the Signalling Gateway can modify its lower layers without impacting the ISTP-Users.

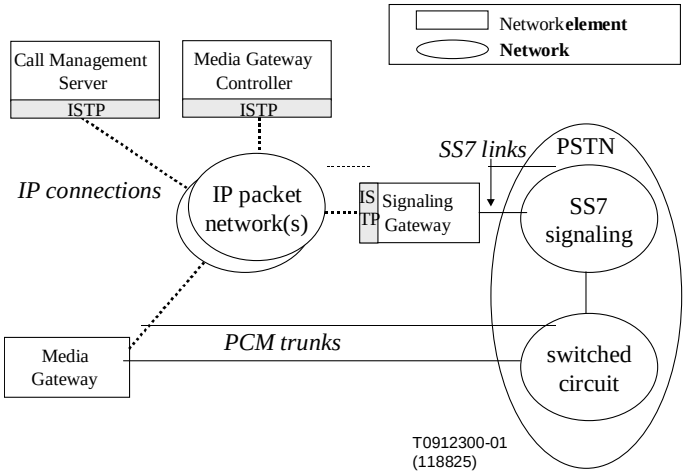


Figure 4: ISTP in decomposed IPCablecom gateway

7.2 Signalling architecture network model

The ISTP focuses on supporting signalling 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 modelling, 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 an 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.

General Terminology: The signalling architecture for ISTP currently consists of three **elements**: Media Gateway Controllers, Call Management Servers, and Signalling Gateways (see figure 2) (see note). Each element can contain one or more separate **nodes** (typically computers), with independent points of failure and IP communication network addresses that cooperate to provide a single function. Note that each node can have one or more addresses (IP addresses or SCTP associations).

NOTE: Note that the concept of an "element" is different from that of a "function", as used in the IPCablecom architecture framework document, ITU-T Recommendation J.160. 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 recommendation allows the logical component parts ("functions") to be combined or further decomposed for physical implementations. In the present 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 the present document.

Thus the term element implements the function as implemented by one or more nodes, while node refers to the individual computer in a redundant set.

- A Signalling Gateway (SG) element is a collection of one or more Signalling Gateway Nodes (SGN). The function of the Signalling Gateway element is to allow for the interworking of the IP-based IPCablecom network with the existing PSTN using SS7 signalling. It provides for the transport of higher level SS7 signalling 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 - the other parameters are known to the SG - 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 communication addresses within the IP network. For the remainder of the present document the terms "Signalling Gateway" or "SG" shall be inferred to mean a "Signalling Gateway Element". Signalling Gateway nodes will be referred to as such using the acronym "SGN". A signalling 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 communication addresses within the IP network. For the remainder of the present 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 to implement IN based services such as number portability, freephone etc. Each CMSN has one or more unique IP communication addresses within the IP network. For the remainder of the present 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 Signalling Gateway appears as a single point code to the SS7 network, where it is viewed as a "signalling endpoint". The SG will manage the transfer of the appropriate messages to the correct ISTP-User element based on 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 PBX "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, this may expose the total network to a software replacement failure.

7.3 Distribution Model

The architecture distribution 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 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, and where possible, stable calls may be maintained in the event of some single failures. 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-signalling layer.

Figure 5 shows a fully distributed and redundant IPCablecom gateway, including the Media Gateway components. In figure 5, ISTP would be used for signalling 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 signalling performance and reliability to the SS7 network. Also, where these requirements can be relaxed in implementation, the model resolves to a simpler subset that is supported by ISTP. Note that:

- every MGC element must be able to take control of any MG;
- only one MGC element at a time is allowed to control a trunk or set of trunks;
- all MGC nodes of an MGC element must be able to control the same set of trunks and one MGC node must potentially recover a stable call in the event of another MGC node failure;
- every SG node must be able to send and receive SS7 messages to every MGC or CMS node;
- The MTP SLS values are distributed according the load-sharing principles of the SS7 network for linksets, i.e. every SGN receives only a subset of the possible SLS values;
- Failure of an SG node that terminates SS7 links, this requires the SS7 network to perform a change-over procedure to redistribute the SLS values;
- communication between MGC and CMS is outside the scope of the present document.

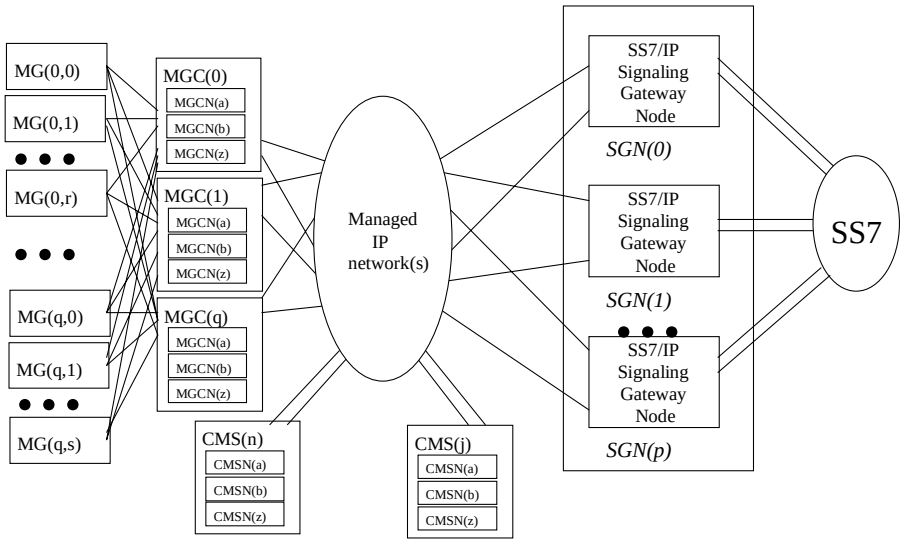


Figure 5: Architecture model of a fully distributed IPCablecom Gateway employing n+k redundancy

7.4 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. Reference may be made to the relevant SS7 standards for guidance in performance budgets.

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 shall:

- meet user expectations of one to two seconds for set up on national communications;
- meet user expectations of 2,5 s to 5 s on international communications.

In order to meet these user expectations for communication set up, which may consist 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 time critical SS7 ISUP events in under 50 ms, and
- process TCAP messages in less than 75 ms.

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

- A sub-layer protocol that:
  - is reliable;
  - is real-time; and
  - 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.
- Signalling messages can not be delayed by other IP traffic; this requires either a dedicated IP network (for signalling or equivalent QoS provisioning to guarantee timely delivery.

7.5 Protocol stack

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

The ISTP resides in the MGC, CMS and SG elements. Figure 3 shows the protocol stack model for ISTP within an IPCablecom SS7 Signalling Gateway and an IPCablecom node.

ISTP requires a reliable underlying transport mechanism. Although ISTP can run over either TCP or SCTP, the Stream Control Transport Protocol (SCTP) as defined in the IETF SIGTRAN working group is preferred. SCTP offers the following features:

- explicit packet-oriented delivery (not byte-oriented);
- sequenced delivery of user messages within multiple streams; although SCTP support an option for order-of-arrival delivery of individual user messages, this ordering shall be mandatory for ISUP messaging;
- optional multiplexing of several user messages destined for the same SCTP association into one SCTP datagram as different DATA chunks, up to the maximum allowable packet length (MTU);
- network-level fault tolerance through support of multi-homing at either or both ends of an association;
- resistance to flooding and masquerade attacks; and
- 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 signalling. Annex A documents how to use SCTP as the reliable transport for ISTP.

8 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 Signalling 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 communication addresses in the IPCablecom network. It will then create an ISTP packet containing the signalling message data and ISTP header data, and send it to the selected node in the IPCablecom network.

From the perspective of an IPCablecom network, the Signalling 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 or TCAP message and send it to the SS7 network.

8.1 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 (SSN), MGC identifiers, and IP communication addresses. In addition, ISTP adds a new numbering unit visible to ISTP nodes, the Circuit Identity (CID). An SS7 trunk is identified by a Circuit Identification Code (CIC), the other end's signalling point code and the network identity. The CIC is created by a joint operator negotiation, and is assigned as an identity to be used between a gateway SS7 end-point node and an SS7 node at the "other end"; thus it may be duplicated within a SG, and it does not uniquely identify a trunk by itself. The CID, that is a combination of the IPCablecom gateway's point code and the Media Gateway's PSTN trunk connection to which it is assigned. This 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, (typically a trunk group of at least one DS-0), is allocated to one and only one MGC element (although the MGC itself can consist of multiple redundant MGCN nodes). Thus all ISUP messages with their CICs are routed over one of the multiple IP connections between the SG and the MGC element that controls that CIC.

Since trunks are fixed in the SS7 network and the MG, and CIDs 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 circuits in a DS-1, a **range** of sequentially numbered circuits would typically be used in allocation and provisioning messages.

Regarding TCAP messages the following should be noted:

- According to the ISTP architecture as specified in the present document, only one IPCablecom element is allowed to register at the Signalling Gateway for a specific SCCP Subsystem.
- Transaction ID's (TID) need to be unique only within an SCCP Subsystem.

Therefore it is the sending CMS element that has to guarantee the uniqueness of the Originating Transaction ID (OTID) over all its nodes. It is assumed that the sending CMS node uses a fixed part of the OTID to uniquely identify itself and the remaining part to uniquely identify the transaction. The SG element/node is informed about length and value of this fixed part used for CMS node identification during the registration process of the CMS node for the Subsystem.

The Signalling Gateway will use this information to correctly route TCAP responses from the SS7 network to the IPCablecom node that originated the query. TCAP messages that originate from the SS7 network, are sent to a randomly selected node in the IPCablecom element that registered for this subsystem handling, and the distribution of the message from that point in is implementation dependant.

8.1.1 SS7 numbering

ESTI standards define the structure of a SS7 message (see EN 300 356 [1]). An ISUP message has a header portion and a parameters portion. In the header are:

- Trunk Circuit Identification Code (CIC), a 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.
- Signalling Link Selection (SLS) code, not needed by ISTP.
- Network Identifier (NI), Origination Point Code (OPC), and Destination Point Code (DPC).

These are unique SS7 network addresses that identify the message origination or destination signalling point

The structure of the TCAP message is described in ETS 300 287-1 [2]

8.1.2 IPCablecom numbering

All ISTP elements names are encoded as e-mail addresses as defined in IETF RFC 821. In these addresses, the domain name identifies the network where the ISTP element is attached. If a unique URL name is given for the ISTP element, a DNS type lookup can be used to initially discover the IP communication addresses of the ISTP nodes- note that this is an option and not a mandatory implementation.

Both components must be case insensitive.

An example of MGC name is:

MGC1@mgc.whatever.net	A Media Gateway Controller node for the "www.whatever.net" network. Note that this is not a URL, but simply a unique text string in a network identified by a URL. The CMS and SG can also be uniquely identified by such means.

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 communication 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 IETF RFC 791.

8.1.3 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. This numbering identifies the circuit being reserved, in use or being disconnected and usually rides a DS1 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 point code and PSTN trunk (CIC).

8.2 Message distribution

ISUP messages destined to the MGCs are routed from SS7 to ISTP elements by mapping the CID to an IP communication address associated with the corresponding MGC node. TCAP queries from the CMS or MGC are routed transparently to the SS7 network, as the sending CMS or MGC could be identified later on using part of the information contained in the responding transaction ID (was OTID in the query) along with information given to the Signalling Gateway during the registration process. Therefore the Signalling Gateway keeps no knowledge at all about TCAP messages sent.

Some messages are internal to ISTP and are routed or broadcast by the SG using IP messaging to all ISTP nodes sharing a point code. This includes maintenance messages, configuration messages, and congestion messages, that is, messages either from the SS7 network or internal status messages that may impact all the MGCs or CMSs.

NOTE 1: The word "IP communication" is often used in the present document, almost as if an actual path exists between IP network elements or nodes. In reality, since the IP network is a packet network, the communication is likely either by a socket for TCP based implementations using an IP address, or an association for SCTP based implementations this can in some implementations handles multiple IP addresses at either one or both ends of the communication.

NOTE 2: While "IP addressing" is often used in the present document, for SCTP an SCTP association is needed. A more general term "IP communication address" or just "communication address" will be used to mean either IP address or SCTP association, but where IP address is used, SCTP associations can be used instead.

8.3 Dynamic Mapping

One function of the ISTP is to dynamically map the target address between the SS7 and IP-based IPCablecom networks for ISUP messages. From the SS7 network, given a CIC, a DPC, OPC and an NI (this is the CID used in IPCablecom) in an incoming SS7 network ISUP message, it will find a target MGC element name. It will then find the MGC Node's IP address, or SCTP association if SCTP is used, from an ordered list of MGC Nodes and attempt to 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, a fixed portion of the originating TCAP transaction ID is used to identify the MGC/CMS name and IP communication address of the node initiating the transaction, and forward the TCAP message via the various levels of the SS7 stack and the SS7 network to the target point code; it will also return replies to the correct sender. This mapping is kept as long as the MGC/CMS node remains registered for a certain SCCP Subsystem. A second function of ISTP is to re-map to redundant or alternate communication addresses upon detection of communication failures. On failures or communication timeouts:

- from the SG side, if a MGC/CMS IP communication fails, it will look up alternate communication addresses (if there are any that have registered) for that MGC/CMS element;
- from the MGC/CMS side, if a SG IP communication fails, the MGC/CMS will look up alternate communication addresses (if there are any that have registered) to the SG element.

Given the performance requirements, ISTP shall avoid using communication addresses that are known to be unavailable, that is, are out of service or have failed a heartbeat test and timed out. Timers may be based on the Recommendations of the TCAP retransmission timers of the interfacing network.

8.4 Relationships

To support the necessary mapping and distribution functions, ISTP assumes a set of relationships that contain "semi-permanent" data. These relationships will typically be in a database and administered by the operations staff and include:

- CID to MGC: this maps a range of CIDs (representing channels (DS0s) to a single MGC element name.
- MGC to IP: this maps an MGC element name to one or more MGC nodes, identified by a communication addresses.
- CMS to IP: this maps a CMS element name to one or more CMS nodes, identified by a communication addresses; the CMS also must know its SSN value for registration of SCCP subsystems.
- SG to IP: this maps the SG element, identified by its point code, to one or mode SG nodes, identified by a communication address.

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

8.5 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, this 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, this 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, this 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, this initializes the node's IP physical and logical communications as well as ISTP data;
- MGC single node initialization, this initializes the node's IP physical and logical communications as well as ISTP data;
- SG single node initialization, this initializes the node's IP physical and logical communications as well as ISTP data;

- ISTP only initialization, this initializes ISTP data;
- IP communication only initialization, this 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, MGC/CMS element, communication addressor 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. This can be administered or supplied by a server on demand (ex: DNS server).

When an element or node restarts, it shall notify **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.

8.6 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 shall automatically switch over to another IP interface (i.e. use an alternate communication address).

ISTP supports two types of recovery: node recovery and element recovery. Node recovery recovers functionality "inside" an element comprised of multiple nodes. Node recovery is primarily used to provide transparent high availability in the event of a single failure of a node in an element set or the single failure of a communication path. Since the nodes are redundant inside an element, with their important data synchronized, one node can take on the activities of a failing node without service interruption. Element recovery moves traffic from one element to a new or alternate element. Element level recovery may lose calls, but provides a way for traffic to be diverted to new MGC elements for a graceful software replacement strategy.

For node recovery, 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(for example, they must share and synchronize state data). Thus, if a far end IP interface on a MGC node or SG node fails, the ISTP must try a second IP communication address; if this fails a third should be tried, etc., up to the optionally provisioned limit of the IP signalling network. Before trying any IP communication address, the ISTP shall check its availability status, this status is kept in internal tables based on the heartbeat status. If the MGC element can not recover a communication, and the node is registered, the SG will discard the messages only after trying all registered MGC nodes and failings.

At the MGC/SG element level, each MGC element can replace another by registering ownership of all the CIC. This element level recovery feature may not have synchronized state data between MGC elements: it is envisioned as a useful part of a software replacement strategy, where you might want to put a new MGC element release on a new set of MGC nodes, and divert traffic to them; if the new node fails, the traffic can automatically fall back to the old release MGC element.

There is only one SG (comprised of possibly multiple SG nodes). If it fails, recovery is beyond the scope of the ISTP, and the MGC needs to initiate appropriate recovery actions (such as providing tones or other failure indications to the end user).

8.7 Dynamic provisioning

The ISTP internal configuration mapping relationships must be dynamically updated without a network restart.

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.

8.8 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 behaviour are beyond the scope of the present document.

8.9 Security

Message authentication will use current state of the art Intranet technology to ensure safe and secure transport of IP messaging. Further security required at ISTP and higher levels is beyond the scope of the present document.

8.10 Maintenance

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

- enable IP communication; this places the IP connect in service and allows traffic;
- disable IP communication; this 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 communication 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 the present document.

ISTP provides no additional requirements on SS7 maintenance. However, there may have to be some coordination of SS7 maintenance with IP maintenance in order to meet the SS7 network requirements. For example, if you disable all IP communications, the SG should notify the SS7 network of that the signalling point is unavailable, as per the relevant SS7 specification.

8.11 Measurement

Operational measurements will be collected; the details on these issues are beyond the scope of the present document.

8.12 Alarms

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

8.13 Congestion

Congestion on the SS7 network will be handled as per SS7 Recommendations 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 from congestion actions. The SG must broadcast a congestion message to all MGC and CMS elements that are registered and active.

8.14 Management of lower layers

ISTP uses SCTP or TCP as its transport layer protocol and must manage the SCTP associations. Refer to clause 10 for SCTP or TCP usage recommendations.

The SG manages the lower layers of SS7 stack. When the status of lower layer objects change, SG is responsible for reporting the changes to MGC. MGC shall respond to the status changes according to the SS7 Recommendation of the interfacing network and react accordingly.

9 Protocol

9.1 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 (it is a subset since it does not include handling of STP functions, only the endpoint functions). These functions include:

- A message distribution function that distributes ISUP and TCAP messages to/from distributed signalling components on the IP 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 ISTP network on the IP side.

9.1.1 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, configuration, and administration 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; and
- close communications.

ISTP is designed to use either TCP/IP or SCTP/IP as its lower layers. The MGC nodes and CMS nodes must initiate the connection to the SG nodes.

The procedures for the setup and takedown of the TCP/IP or SCTP connections are defined in an annex to the present document. Raw format means a message that is the exact SS7 TCAP or ISUP 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. In case of a Signalling Gateway connected to an SS7 network based on ETSI standards, raw format MUST be used. It is therefore required that the IPCablecom nodes comply with the ETSI ISUP and TCAP protocol.

NOTE: Connecting a Signalling Gateway to an SS7 network not according to ETSI standards, is out of scope. Therefore the usage of the "normalized" format is not allowed. This format and subsequent references to it, are kept for compatibility reasons only.

9.1.2 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 ETSI recommendations. The content and the encoding of all parameters used in ISTP are defined in the present document, except for the content of the ISUP and TCAP parameters.

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

When using raw formatting, the TCAP or ISUP content of the SS7 message is conveyed in its native MTP form, as outlined by the SS7specification. This feature is primarily intended to allow the support of differentiation services by vendors in areas where variant or national protocols have information not in the standard SS7 messages, and where this information may be necessary or required by the vendor to implement a feature.

When using normalized formatting, the SS7 content is transferred between IPCablecom element using "standard" SS7 messaging (ex: ANSI or ETSI or ITU standards) and the SS7 network that may use variant protocols (i.e. national variants). The feature is used to eliminate the CMS/MGC vendor from having to deal with such variants.

9.1.3 SS7 Load-sharing and sequencing

In a conventional SS7 application, the MTP Level 3 relies on the upper layers to supply the signalling 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 signalling 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.

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

9.2 Procedures

9.2.1 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 after communication is started among the elements. 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 that uses the DPC, OPC and CIC for ISUP messages;
- provide some validation of the MSUs bound for the SS7 network. That is, only registered elements can access the SS7 network; non-registered IP nodes will not be allowed.

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. This means that each MGC node in a MGC element registers with all the SG nodes (note that the SG implementation may synchronize the registration tables, but all MGC nodes should still register with all known SG nodes using the IP communication address). Thus, if a single MGC node fails, the SG node receiving an ISUP message can look up another MGC node registered for that circuit; if a SG node fails, another SG node can perform the same function since it has identical registration tables. MGC elements are identified by name, and MGC nodes by IP communication address. SG elements are identified by name, and SG nodes by IP communication addresses.

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 communication addresses.

9.2.1.1 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 origination 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 in cases where the SG can support multiple point codes (which is a possible option) it checks multiple point codes;
- 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 registration 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 (note that SG nodes are expected to have synchronized tables- the mechanism for this is outside the scope of the present document;
- 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 a circuit registration acknowledgements with the proper failure indication.

The authentication tables and algorithms for distribution and load sharing of messages to nodes are implementation dependent.

9.2.1.2 Circuit deregistration

The MGC node sends a *circuit deregistration* request to the SG node to indicate that it no longer wishes to reserve the specified circuit range. Parameters of the deregistration request include the MGC name, the gateway point code, the target point code and a CIC range. Note that the SG shall verify that the deregistration of a CIC range shall match the registration rage, or else there will be a mismatch; in such a mismatch case the request shall be rejected.

When the SG node receives a *circuit deregistration* 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 deregistration* acknowledgement with a success indication. If not, it returns a circuit registration acknowledgement with the proper failure indication.

9.2.2 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 within a MGC element is implementation dependent. In addition it is expected that any MGC node that registers with a SG node can handle an incoming ISUP message; any maintenance of call states or other data must be synchronized by the MGC element among all its nodes; any forwarding of messages from one MGC node to another is the responsibility of the MCG.

9.2.2.1 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 (uniquely identified by IP communication address) 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). In addition it is expected that any MGC node that registers with a SG node can handle an incoming ISUP message; any maintenance of call states or other data must be synchronized by the MGC element among all its nodes; any forwarding of messages from one MGC node to another is the responsibility of the MCG.

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

9.2.2.2 Forced exclusive circuit activation

The MGC node sends a *forced exclusive circuit activation* request to the SG when it wishes to send and receive SS7 messages pertaining to the specified circuits, and override any existing activation(s) for the SG. The parameters include the MGC name, the gateway point code, the target point code and CIC range. It is the responsibility of the SG element to internally broadcast this message to its SG nodes.

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 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 a forced exclusive circuit activation acknowledgement with the proper failure indication.

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

The idea is to take out of service a MG circuit or MG element; the MGC is involved since it has to take the circuits out of service in its tables first, and thus this handshake mechanism is required. 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).

9.2.2.3 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 ore more MGC nodes to another. This is a transient activity, typically employed during a software upgrade when you want to shift traffic off a node so you can replace the software without disrupting service. 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 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). This implies that the SG nodes maintain synchronized "maintenance states" within a SG element. 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. It is also assumed that the SG nodes maintain the ISUP circuit states synchronized within a SG element.

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).

9.2.2.4 Circuit deactivation

The MGC node sends a *circuit deactivation* 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 deactivation request also include the MGC name, DPC, the OPC and a CIC range.

When the SG node receives a *circuit deactivation* 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 deactivation* 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. If the MGC deactivates all circuits to the whole MGC element, the situation is analogous to a local exchange going out of service, and the network must wait until the MGC brings the affected circuits back on line.

9.2.3 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 that uses the gateway point code and SSN for TCAP messages to distribute it to the element name that registered for the SSN;
- provide some validation of the MSUs bound for the SS7 network.

All nodes of a CMS/CA element register with the nodes of the SG element for the same subsystem. However, the registration for more than one subsystem is possible 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 PSTN initiated transactions to be forwarded to the CMS/CA on point code and subsystem number basis as specified in the initiating party's address.

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.

9.2.3.1 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. Note that it is assumed that a CMS/CA element uses one or the other format for all communications. For ETSI purposes the CMS/CA node MUST specify "raw" message format. Parameters to the registration request include the gateway point code, the SSN, the node identification that is part of every OTID and the message format, and the IP communication address of the sending CMS (which is in the lower TCP or SCTP layer of the message). 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, that is, a CMS is registered with for SSN;
- 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;
- no other CMS node of this element uses the same node identification value;
- it can support the requested transfer format, in case of an ETSI SG it has to make sure that "raw" format is used.

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.

9.2.3.2 Subsystem transaction deregistration

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

When the SG receives a *subsystem deregistration* 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 deregistration* acknowledgement with a success indication. If not, it returns an acknowledgement with the proper failure indication.

9.2.4 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.

9.2.4.1 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 in the CMS/CA element 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 (TC-BEGIN) and unidirectional (TC-UNI) messages coming from the SS7 network.

If the TCAP message coming from the SS7 network is a response (TC-END) or a conversation (TC-CONTINUE) 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 correlating the subfield representing the node identification in the responding transaction ID (was the OTID assigned by the sending node) with the list of CMS/CA node identifications generated during node registration, thus determining the communication address of the concerned CMS/CA node.

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

9.2.4.2 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.

9.2.4.3 Subsystem deactivation

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 deactivation request also include the DPC, the OPC and the subsystem.

When the SG node receives a *subsystem deactivation* 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 deactivation* 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.

9.2.5 Message transfer

The message transfer procedure is the one that the MGC, the 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.

9.2.5.1 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, NI, 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.

9.2.5.2 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 Originating Transaction ID.

The transaction identifiers are defined to be unique for the duration of the transaction between the SS7 nodes. It is, however, important to recognize that this uniqueness is not required across all SCCP Subsystems handled by the SG element. The uniqueness is only required within every SCCP Subsystem.

When the CMS/CA sends a query message to the SG using the TCAP message transfer procedure, the Originating Transaction ID (OTID) is set to a unique value as defined by the CMS/CA node. The OTID comprises two subfields, the unique node identification that has been negotiated with the SG during subsystem registration and a variable field that allows to distinguish the active transactions originating from that node.

When the CMS/CA responds with either a TC-CONTINUE, TC-END, TC-ABORT, TC-U-ABORT or TC-UNI message to the SG, no special routing based on the transaction ID is required.

When the SG receives a TC-CONTINUE or TC-END message from the SS7 network, it extracts the TCAP responding transaction ID (was the OTID assigned by the sending node) and correlates the subfield representing the node identification with the list of CMS/CA node identifications generated during node registration, thus determining the communication address of the concerned CMS/CA node.

When the SG receives a TC-BEGIN or TC-UNI message from the SS7 network, it sends TCAP Message Transfer to an active CMS node of the CMS/CA element registered for the corresponding SSN. This node is selected using an implementation dependent algorithm.

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

9.3 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.

9.3.1 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 ISTP level 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 shall be disabled within a time period that allows the IPCablecom network to meet its stated availability requirements.

9.3.2 Signalling gateway procedures

9.3.2.1 Signalling point accessibility

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

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

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

9.3.2.2 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 an SCCP subsystem on a remote signalling point where there is a concerned CMS (i.e. CMSs that have registered subsystem with the affected signalling point), it sends a *subsystem inaccessible* indication to each concerned CMS node. According to the SS7 Recommendations, it also stops transferring messages from the CMS to the affected subsystem.

If a subsystem becomes accessible and there are some concerned CMSs, the signalling 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 CMSs.

9.3.2.3 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 Recommendations), 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.

9.3.2.4 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 an ISTP node it deactivates and deregisters all circuits and subsystems with that ISTP element, and discards any subsequent SS7 messages that 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.

9.3.2.5 Congestion on the SS7 network

If the SG detects the congestion of a signalling point by receiving a TFC message, it sends a *signalling point congestion* indication to the concerned MGC and CMS nodes.

The SG shall provide a mechanism for detection of the end of a congestion status. 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. When the congestion status ends, the SG sends a *local congestion* indication to all connected MGC and CMS nodes.

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

9.3.3 MGC and CMS procedures

9.3.3.1 Signalling point accessibility

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

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

9.3.3.2 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 signalling 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.

9.3.3.3 Signalling 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 deregistered.

If the MGC or CMS node was providing service for some circuits or subsystem transactions, it likely tries to re-establish service to minimize the downtime associated with the failure by implementation dependent node recovery actions, and by attempting to re-establish the connection with the SG.

The specific recovery procedures are implementation specific.

9.3.3.4 SS7 Network congestion

When an MGC or CMS node receives a *signalling point congestion* indication, it marks the destination as congested. It also treats this message as an MTP-STATUS with e as defined in the various SS7 Recommendations.

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

9.3.3.5 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 discarding messages until the congestion is ended.

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

9.4 Message format

The table below illustrates the format of an ISTP message.

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.

9.4.1 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.

Message type	ID	Nature	Notes
Circuit-Registration	0	Req, Rsp	
Circuit-Deregistration	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-Deregistration	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.
Inaccessible-Point-Inaccessible	16	Ind	Only sent by the SG.
Accessible-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.
Congestion-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.

9.4.2 Message nature

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

9.4.3 Parameters

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

Parameter Name	ID	Format	Reference
affectedPointCode	0	pointCode	clause 9.4.3.11
calledPartyAddress	1	sccpPartyAddress	clause 9.4.3.16
callingPartyAddress	2	sccpPartyAddress	clause 9.4.3.16
cic	3	cic	clause 9.4.3.1
circuitRange	4	circuitRange	clause 9.4.3.3
cmsName	5	asciiString	clause 9.4.3.1
congestionLevel	6	integer (1 octet)	clause 9.4.3.6
destinationType	7	integer (1 octet)	clause 9.4.3.4
inaccessibilityReason	8	integer (1 octet)	clause 9.4.3.5
isupClientReturnValue	9	integer (1 octet)	clause 9.4.3.7
isupTransferFormat	10	integer (1 octet)	clause 9.4.3.8
mgcName	11	asciiString	clause 9.4.3.1
normalizedISUPMsg	12	stream	clause 9.4.3.9
normalizedTCAPMsg	13	stream	clause 9.4.3.10
rawISUPMsg	14	stream	clause 9.4.3.13
rawTCAPMsg	15	stream	clause 9.9.4.3.14
routingLabel	16	routingLabel	clause 9.4.3.15
ssn	17	integer (1 octet)	clause 9.4.3.6
subsystem	18	subsystem	clause 9.4.3.18
subsystemActionReturnValue	19	integer (1 octet)	clause 9.4.3.19
tcapTransferFormat	20	integer (1 octet)	clause 9.4.3.20
transactionIdentifier	21	integer (4 octets)	clause 9.4.3.6 (not used)
nodeIdentification	22	integer (2 octet)	clause 9.4.3.6
-- reserved --	65535	n/a	Reserved for future expansion.

9.4.3.1 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.

9.4.3.2 cic

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

9.4.3.3 CircuitRange

This parameter contains point codes and circuit identification that identify a range of circuits.

It has a length of 10 octets total.

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.
networkIndicator	integer	1	The NI value from the MTP routing label.
cicLowerBound	cic	2	The lower CIC value of the sieve, inclusive.
cicUpperBound	cic	2	The upper CIC value of the sieve, inclusive.

9.4.3.4 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:

This value MUST to be set to "3" in an ETSI environment.

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

9.4.3.5 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:

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

9.4.3.6 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 65 535 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.

9.4.3.7 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:

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

9.4.3.8 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:

This value MUST be set to "0" in an ETSI environment.

Value	Definition
0	raw ISUP messages
1	normalized ISUP messages

9.4.3.9 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 ISUP SS7 Recommendations.

In an ETSI Environment "NormalizedISUPMsg" is not be used.

9.4.3.10 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 SS7 TCAP Recommendations. The parameters used within the component sections of the TCAP message follow the respective TCAP protocol Recommendations of the messages being conveyed (i.e. AIN, GSM, IS-41, LIDB, etc.).

In an ETSI Environment "NormalizedTCAPMsg" is not be used.

9.4.3.11 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 (24 bits) 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.

ETSI 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 Recommendations, with the first octet to be transmitted stored in the first octet of the ISTP parameter.

9.4.3.12 QualityOfService

This parameter contains the information on the quality of service requirements.

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.

9.4.3.13 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 ETSI SS7 ISUP Recommendations.

9.4.3.14 rawTCAPMsg

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

9.4.3.15 routingLabel

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

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 signalling link selection field.

9.4.3.16 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.

Field name	Type	Size	Notes
addressIndicator	integer	1	The address indicator format can be found below.
ssn	integer	1	The subsystem number.
networkIndicator	integer	1	The NI value from the MTP routing label.
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.

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 ETSI SS7 implementations.

9.4.3.17 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 Recommendations. The encoding of the parameters using this format is also specified in the respective SS7 Recommendations.

9.4.3.18 subsystem

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

Field name	Type	Size	Notes
networkIndicaton	integer	1	The NI value from the MTP routing label.
localPointCode	pointCode	3	The point code of the CMS/CA.
ssn	integer	1	The subsystem number.
nodeIdentification	integer	2	The two most significant bytes of the OTID.

9.4.3.19 subsystemActionReturnValue

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

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
7	node identifier not unique within element

9.4.3.20 tcapTransferFormat

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

In an ETSI Environment this parameter MUST be set to "0".

Value	Definition
0	raw TCAP messages
1	normalized TCAP messages

9.5 Messages

This clause 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 clause 9.4.1. The encoding of the parameters is found in the previous clauses.

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, but mandatory parameters have to precede optional ones.

9.5.1 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:

9.5.1.1 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:

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.

9.5.1.2 Circuit deregistration

The MGC sends the SG a circuit deregistration 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.

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

9.5.1.3 Circuit activation

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

The circuit activation message contains the following information:

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.

9.5.1.4 Forced exclusive circuit activation

The MGC sends the SG a forced exclusive circuit activation request to indicate that the specified entry shall 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.

9.5.1.5 New work circuit activation

The MGC sends the SG a new work circuit activation request to indicate that the specified entry shall 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.

9.5.1.6 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.

9.5.1.7 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.

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

9.5.1.8 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.

9.5.2 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:

9.5.2.1 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:

Parameter name	REQ	RSP	Notes
cmsName	M	M	The name of the CMS/CA element.
subsytem	M	M	The subsystem to register.
tcapTransferFormat	M	M	Enumeration identifying the preferred format of the IP-bound TCAP messages.
nodeIdentification	M	M	The unique identification of the node to be used as part of the OTID
subsystemActionReturnValue	n/a	M	The return code for the operation.

9.5.2.2 Subsystem deregistration

The CMS/CA sends the SG a subsystem deregistration 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 SubsystemActionReturnValue parameter.

Parameter name	REQ	RSP	Notes
cmsName	M	M	The name of the CMS/CA element.
subsystem	M	M	The subsystem to deregister.
nodeIdentification	M	M	A unique identification of the node to be used as part of the OTID
subsystemActionReturnValue	n/a	M	The return code for the operation.

9.5.2.3 Subsystem activation

The CMS/CA sends the SG a subsystem activation request to indicate that the specified entry shall 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:

Parameter name	REQ	RSP	Notes
cmsName	M	M	The name of the CMS/CA element.
subsystem	M	M	The subsystem to register.
nodeIdentification	M	M	A unique identification of the node to be used as part of the OTID.
subsystemActionReturnValue	n/a	M	The return code for the operation.

9.5.2.4 Exclusive subsystem activation

The CMS/CA sends the SG an exclusive subsystem activation request to indicate that the specified entry shall 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.

9.5.2.5 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.

9.5.2.6 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.

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

9.5.3 Message transfer

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

9.5.3.1 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.

In an ETSI Environment only the parameter rawISUPMsg MUST be used.

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.

9.5.3.2 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.

In an ETSI Environment only the parameter rawTCAPMsg MUST be used.

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.
normalizedTCAPMsg	C	The normalized TCAP message to transfer.
rawTCAPMsg	C	The raw (original) TCAP message to transfer.

9.5.4 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 signalling 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 6level. If congestion is experienced between the MGC or the CMS and the SG, from the SG perspective, there are no procedures that are required.

9.5.4.1 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.

9.5.4.2 Signalling point inaccessible

The SG sends the MGC or the CMS a s*ignalling 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 that has no defined route set (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 *signalling 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:

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.

9.5.4.3 Signalling point accessible

The SG sends the MGC and the CMS a *signalling 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 *signalling 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:

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

9.5.4.4 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 that 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:

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

9.5.4.5 Subsystem accessible

The SG sends the CMS a *signalling 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:

Parameter name	IND	Notes
subsystem	M	The destination subsystem.

9.5.4.6 Signalling point congestion

The SG sends a *signalling 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 may contain the following information:

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

9.5.4.7 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 may contain the following information:

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

9.5.4.8 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.

9.5.4.9 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.

Annex A (informative): 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 clause.

A.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 ISTP. This clause 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 signalling traffic only. Sharing IP connection with other traffic over the signalling links can result in performance and reliability degradation.

A.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 signalling 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 shall support the assignment of signalling traffic into streams within an SCTP association. Traffic that requires sequencing must be assigned to the same stream. To accomplish this, MTP3-User traffic shall be assigned to individual streams based on the SLS value in the MTP3 Routing Label.

A.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 shall 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 MGC or CMS/CA node is encountering congestion, the SG shall 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 node, 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.

A.2 TCP usage recommendations

TCP can be used in IPCablecom as a transport mechanism as an option. However, there are a number of considerations regarding the use of TCP/IP in a near real-time context for the transportation of ISTP. This annex 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 signalling traffic only. Sharing IP connection with other traffic over the signalling links can result in performance and reliability degradation.

A.2.1 Delaying of packets

TCP/IP 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 Signalling 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 disabled by issuing the following system call on the socket's file descriptor:

EXAMPLE: 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.

A.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 Signalling 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: 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.

A.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: Setting the SO_LINGER time Option

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

Annex B (informative): ISTP message flows and timer definitions

B.1 Timers

This clause defines the timers used by the MGC and SG to monitor the responses of ISTP messages. The present document does not mandate the action to take when a timer expires. All timers are user configurable.

Table B.1

Timer id	Default Time-out	Range	Purpose	Started when the following messages are sent	Stopped when
Session-timer	30 s	1 s to 120 s	Monitor session-based messages.	Circuit-Registration Circuit-Deregistration Circuit-Activation Circuit-Deactivation Exclusive-Circuit-Activation Forced-Circuit-Deactivation New-Work-Circuit-Activation New-Work-Circuit-Deactivation Subsystem-Registration Deregistration Activation; Exclusive-Subsystem-Activation Forced-Subsystem-Activation	Corresponding ACK or NACK messages are received
Transaction-timer	4 s	1 s to 30 s	Monitor transaction-based messages	ISUP-Message-Transfer TCAP-Message-Transfer	Corresponding ACK or NACK messages are received
Heartbeat-Timer	1 s	10 ms to 60 s	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 shall also be raised in accordance with standard error practices.

B.2 MGC requests ISUP service procedure

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

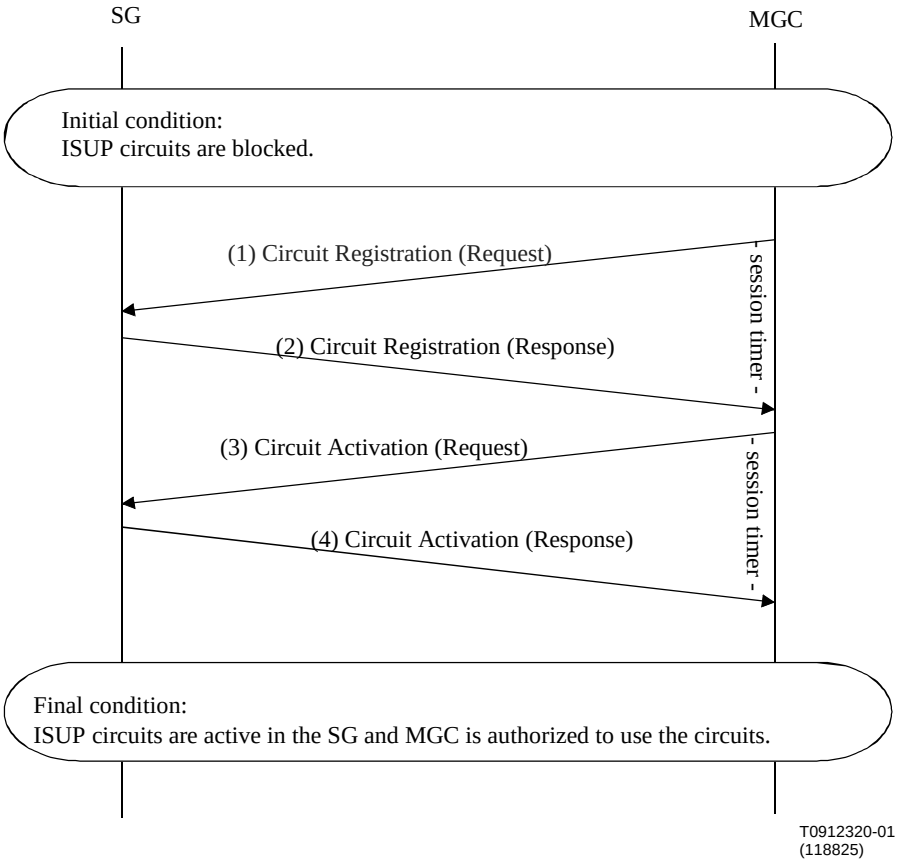


Figure B.1: MGC requests ISUP service

- MGC node sends a Circuit Registration request to the SG node to reserve a group of circuits for its use. The session timer is started to monitor the response from SG node. The request specifies the IP communication address of MGC node, the circuit range, and ISUP message format, raw or normalized ISUP messages. Note that the gatewayPointCode 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 shall fill in the gatewayPointCode field in the circuitRange parameter with its point code and isupClientReturnValue parameter with proper return value. Upon receiving this message, MGC node cancels the session timer. If the timer expires before receiving a response from SG node, the MGC node shall take proper action.

- If the return code in the Circuit Registration response is *successful_and_inactive* and the MGC node is ready to service the ISUP messages on the circuits, it sends a Circuit Activation request to SG node to activate the circuits. One or more session timers are started to monitor the response from SG.

- The SG node sends a Circuit Activation response to the MGC node. If the isupClientReturnValue field is set to *successful_and_active*, the MGC node is granted the right to use the specified circuits. Upon receiving this message, the MGC node cancels the session timer. If the timer expires before receiving a response from SG node, the MGC node shall take proper action.

B.3 MGC terminates ISUP service procedure

This scenario describes the deregistration and deactivation process as an MGC terminates the ISUP service from a SG.

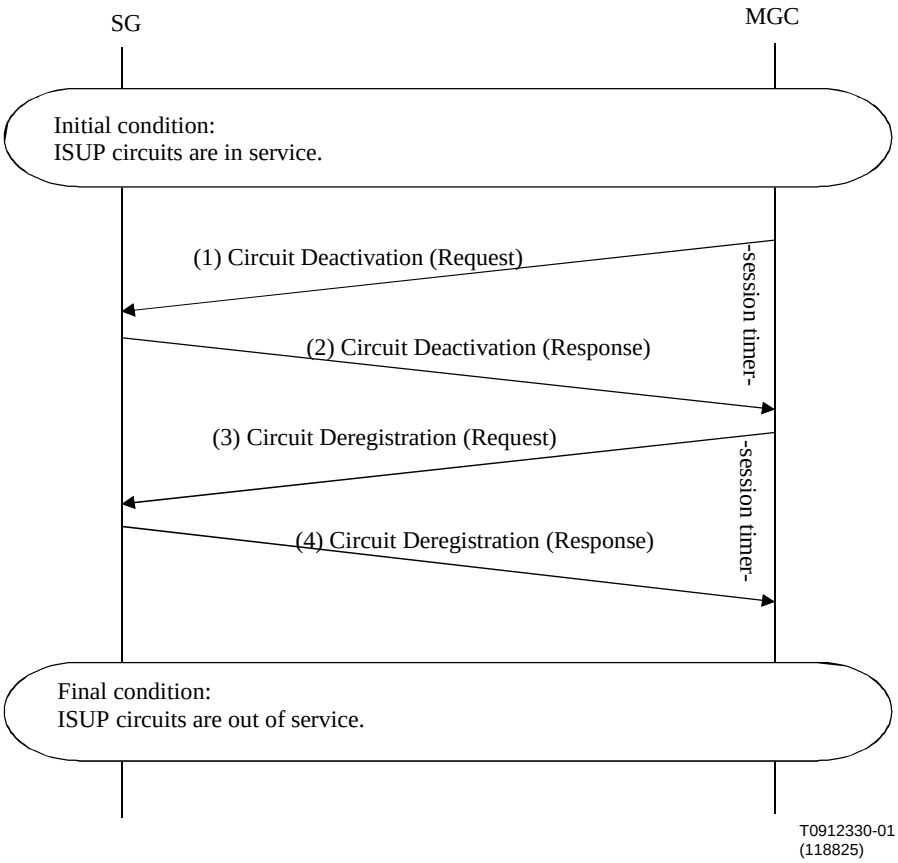


Figure B.2: MGC terminates ISUP service

- MGC sends a Circuit Deactivation request to SG to deactivate the specified circuits. Once a circuit is deactivated, SG shall discard any ISUP 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* shall 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 deregistration. If the deregistration is successful, the *isupClientReturnValue* shall 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.

B.4 Residential CA requests TCAP service procedure

This scenario describes the registration and activation process when a residential Ca, that is a call agent for a subscriber (the CMS), requests the TCAP service from a SG.

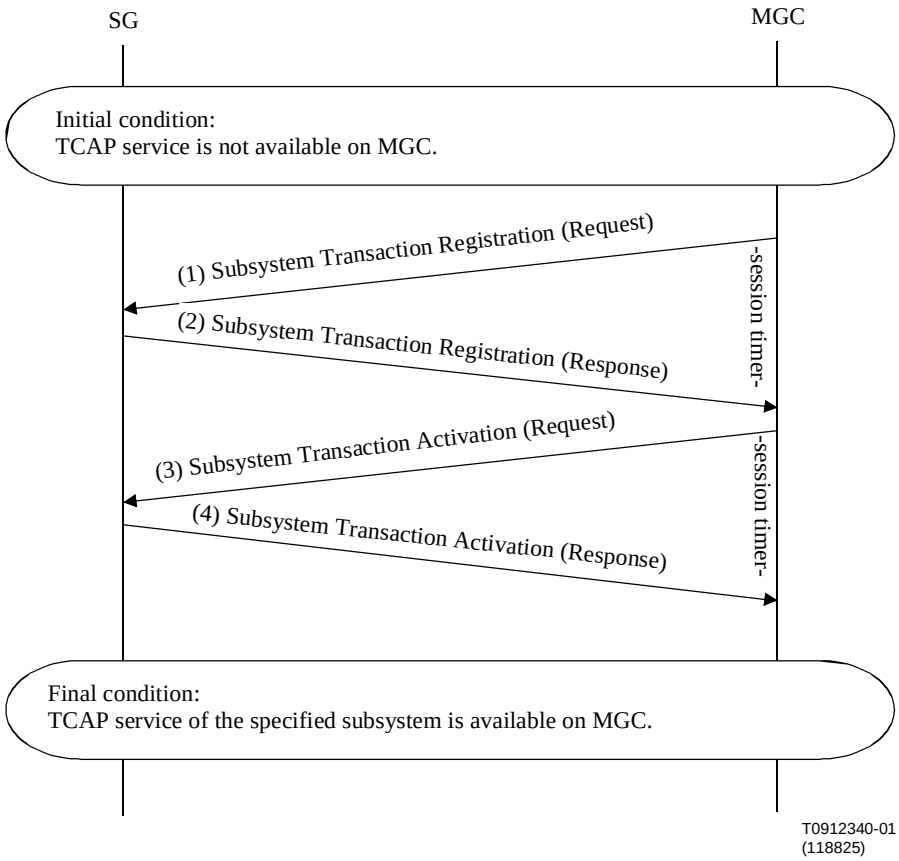


Figure B.3: MGC requests TCAP service

- 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 subsystemActionReturnValue 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 subsystemActionReturnValue 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.

B.5 Residential CA terminates TCAP service procedure

This scenario describes the deregistration and deactivation process as a residential CA terminates the TCAP service from a SG.

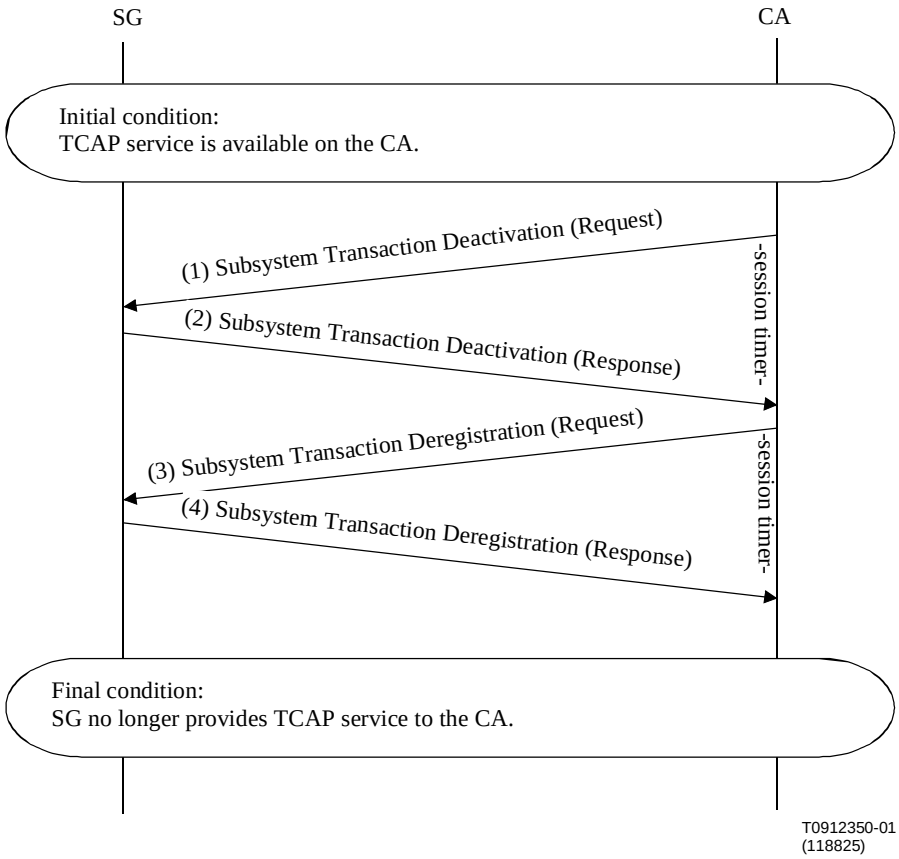


Figure B.4: CA terminates TCAP service

- 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 subsystemActionReturnValue 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 Deregistration 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 Deregistration response with the subsystemActionReturnValue 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.

B.6 MGC failover procedure

This flow demonstrates the failover procedure when the MGC runs in redundant mode. . MGC1 and MGC2 are both nodes of the MGC, and the particular implementation shows an active and standby (redundant) configuration. Other configurations arte possible as well.

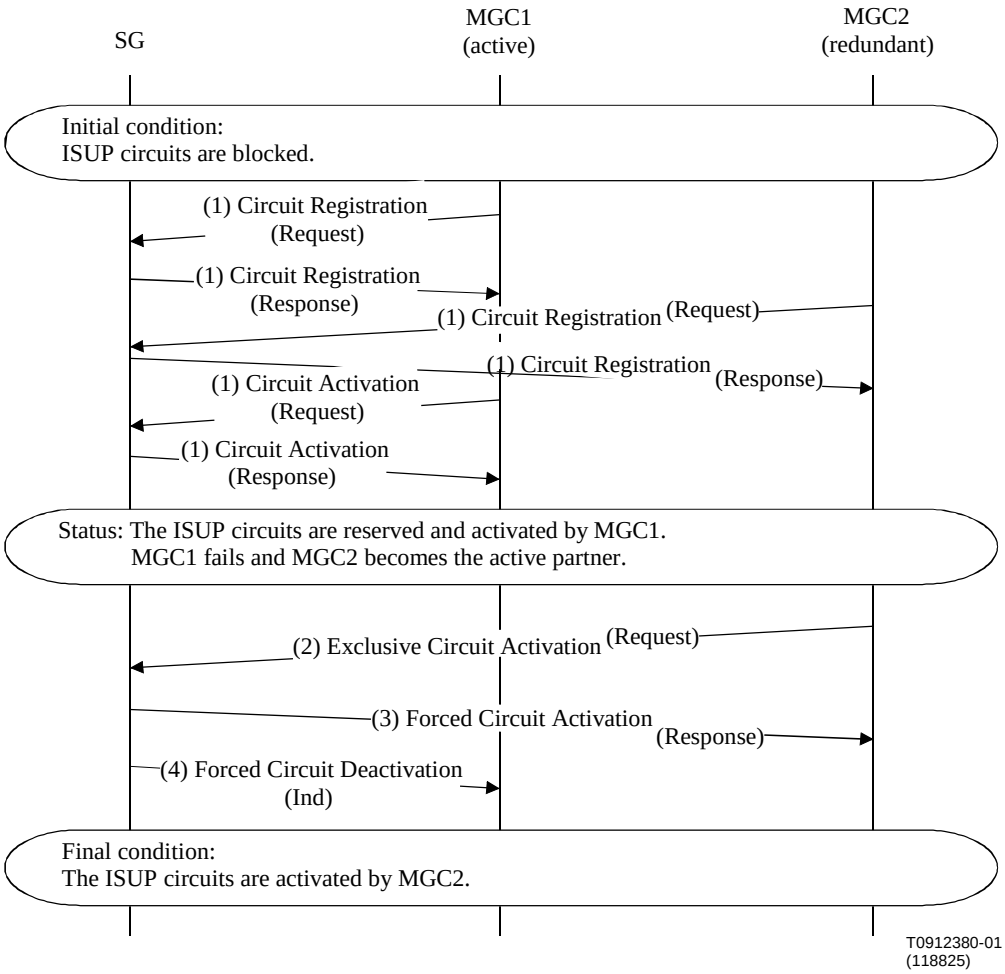


Figure B.5: MGC failover procedure

- MGC1 and MGC2 are a redundant pair to serve the same set of ISUP 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.

B.7 MGC switchover procedure

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

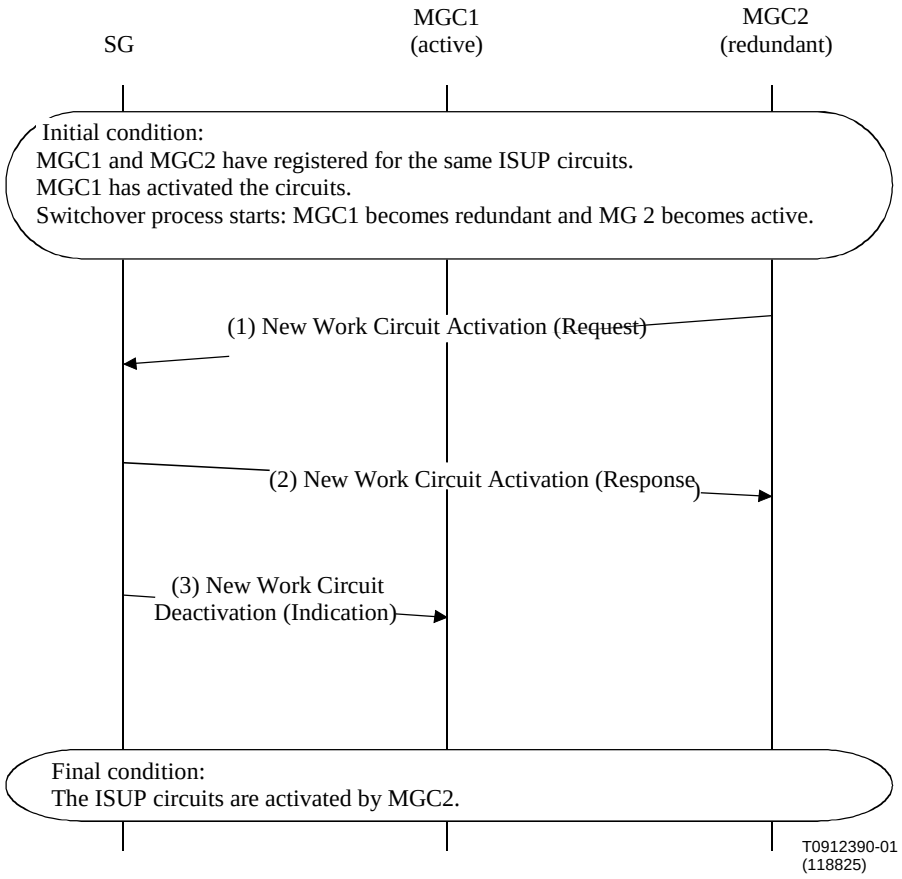


Figure B.6: MGC switchover procedure

- 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 messages for the existing communications to MGC1 and ISUP 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.

Annex C (informative): Bibliography

- ETSI EN 302 097: "Integrated Services Digital Network (ISDN); Signalling System No.7 (SS7); ISDN User Part (ISUP); Enhancement for support of Number Portability (NP) [ITU-T Recommendation Q.769.1 (2000), modified]".
- ETSI EN 300 008-1: "Integrated Services Digital Network (ISDN); Signalling System No.7; Message Transfer Part (MTP) to support international interconnection; Part 1: Protocol specification [ITU-T Recommendations Q.701, Q.702, Q.703, Q.704, Q.705, Q.706, Q.707 and Q.708 modified]".
- ETSI EN 300 009-1: "Integrated Services Digital Network (ISDN); Signalling System No.7; Signalling Connection Control Part (SCCP) (connectionless and connection-oriented) to support international interconnection; Part 1: Protocol specification [ITU-T Recommendations Q.711 to Q.716 (1996), modified]".
- IEEE 802.3: "Computer Society/Local and Metropolitan Area Networks".
- IETF RFC 791: "Internet Protocol".
- IETF RFC 821: "Simple Mail Transfer Protocol".
- IETF RFC 2960: "Stream Control Transport Protocol (SCTP)", Dec. 2000.
- IETF RFC 3309: "Stream Control Transmission Protocol (SCTP) Checkshum Change".
- ITU-T Recommendation J.112 (including annexes and published Amendments): "Transmission systems for interactive television services".
- ITU-T Recommendation J.160: "Architectural framework for the delivery of time critical services over cable television networks using cable modems".
- ITU-T Recommendation Q.704 (1996): "Signalling network functions and messages".
- ITU-T Recommendation Q.711 (1996): "Functional description of the Signalling Connection Control Part".
- ITU-T Recommendation Q.712 (1996): "Definition and function of Signalling Connection Control Part messages".
- ITU-T Recommendation Q.713 (1996): "Signalling Connection Control Part formats and code".
- ITU-T Recommendation Q.714 (1996): "Signalling Connection Control Part procedures".
- ITU-T Recommendation Q.761 (1999): "Signalling system No. 7 - ISDN User Part functional description".
- ITU-T Recommendation Q.762 (1999): "Signalling System No. 7 - ISDN User Part general functions of messages and signals".
- ITU-T Recommendation Q.763 (1999): "Signalling system No. 7 - ISDN User Part formats and codes".
- ITU-T Recommendation Q.764 (1999): "Signalling system No. 7 - ISDN User Part signalling procedures".
- ITU-T Recommendation Q.771 (1997): "Functional description of transaction capabilities".
- ITU-T Recommendation Q.772 (1997): "Transaction capabilities information element definitions".
- ITU-T Recommendation Q.773 (1997): "Transaction capabilities formats and encoding".
- ITU-T Recommendation Q.774 (1997): "Transaction capabilities procedures".
- ITU-T Recommendation Q.775 (1997): "Guidelines for using transaction".

History

Document history		
V1.1.1	November 2002	Publication