INTERNET-DRAFT
Internet Engineering Task Force

Issued: 30 June 2002
Expires: 30 December 2002

J. Loughney (Editor)
Nokia
G. Sidebottom
gregside Consulting
L. Coene, G. Verwimp
Siemens
J. Keller
Tekelec
B. Bidulock
OpenSS7 Corporation

Signalling Connection Control Part User Adaptation Layer (SUA)

Status of This Memo

Abstract

This Internet Draft defines a protocol for the transport of any Signalling Connection Control Part-User signalling (e.g., Transaction Capabilities Protocol, Radio Acccess Network Application Protocol, etc.) over IP using the Stream Control Transport Protocol. The protocol should be modular and symmetric, to allow it to work in diverse architectures, such as a Signalling Gateway to IP Signalling Endpoint architecture as well as a peer-to-peer IP Signalling Endpoint architecture. Protocol elements are added to allow operation between peers in the Signaling System No.7 and IP domains.

1. Introduction

This draft defines a protocol for the transport SS7 SCCP [ANSI SCCP] [ANSI SCCP] Users (i.e. TCAP, RANAP, etc.) signalling messages over IP using the Stream Control Transmission Protocol (SCTP) [2960]. This protocol would be used between a Signalling Gateway (SG) and Signaling Endpoint located in an IP network. Additionally, the protocol can be used to transport SS7 SCCP users between two signaling endpoints located within an IP network.

1.1 Scope

There is on-going integration of SCN networks and IP networks. Network service providers are designing all IP architectures that include support for SS7 and SS7-like signalling protocols. IP provides an effective way to transport user data and for operators to expand their networks and build new services. In these networks, there is need for interworking between the SS7 and IP domains [2719].

This document details the delivery of SCCP-user messages (MAP & CAP over TCAP [ANSI TCAP] [ITU TCAP], RANAP [RANAP], etc.) and new 3rd Generation network protocol messages over IP between two signalling endpoints. Consideration is given for the transport from an SS7 Signalling Gateway (SG) to an IP signalling node (such as an IP-resident Database) as described in the Framework Architecture for Signalling Transport [2719]. This protocol can also support transport of SCCP-user messages between two endpoints wholly contained within an IP network.

The delivery mechanism addresses the following criteria:

* Support for transfer of SCCP-User Part messages (TCAP, RANAP, etc.)
* Support for SCCP connectionless service.
* Support for SCCP connection oriented service.
* Support for the seamless operation of SCCP-User protocol peers.
* Support for the management of SCTP transport associations between a SG and one or more IP-based signalling nodes).
* Support for distributed IP-based signalling nodes.

* Support for the asynchronous reporting of status changes to management.

1.2 Terminology

Signalling Gateway (SG) - Network element that terminates SCN signalling and transports SCCP-User signalling over IP to an IP signalling endpoint. A Signalling Gateway could be modeled as one or more Signalling Gateway Processes, which are located at the border of the SS7 and IP networks. Where an SG contains more than one SGP, the SG is a logical entity and the contained SGPs are

assumed to be coordinated into a single management view to the SS7 network and to the supported Application Servers.

Application Server (AS) - A logical entity serving a specific Routing Key. An example of an Application Server is a virtual IP database element handling all requests for a SCCP-user. The AS contains a set of one or more unique Application Server Processes, of which one or more is normally actively processing traffic.

Application Server Process (ASP) - An Application Server Process serves as an active or backup process of an Application Server (e.g., part of a distributed signalling node or database element). Examples of ASPs are MGCs, IP SCPs, or IP-based HLRs. An ASP contains an SCTP end-point and may be configured to process traffic within more than one Application Server.

IP Server Process (IPSP) - A process instance of an IP-based application. An IPSP is essentially the same as an ASP, except that it uses SUA in a peer-to-peer fashion. Conceptually, an IPSP does not use the services of a Signalling Gateway.

Signalling Gateway Process (SGP) - A process instance of a Signalling Gateway. It serves as an active, load-sharing or broadcast process of a Signalling Gateway.

Signalling Process - A process instance that uses SUA to communicate with other signalling process. An ASP, a SGP and an IPSP are all signalling processes.

Association - An association refers to an SCTP association. The association provides the transport for the delivery of SCCP-User protocol data units and SUA layer peer messages.

Routing Key - The Routing Key describes a set of SS7 parameters and/or parameter-ranges that uniquely defines the range of signalling traffic configured to be handled by a particular Application Server. An example would be where a Routing Key consists of a particular SS7 SCCP SSN plus an identifier to uniquely mark the network that the SSN belongs to, for which all traffic would be directed to a particular Application Server. Routing Keys are mutually exclusive in the sense that a received SS7 signalling message cannot be directed to more than one Routing Key. Routing Keys can be provisioned, for example, by a MIB or registered using SUA's dynamic registration procedures. Routing keys MUST NOT span multiple network appearances.

Routing Context - An Application Server Process may be configured to process traffic within more than one Application Server. In this case, the Routing Context parameter is exchanged between the SGP and the ASP (or between two ASPs), identifying the relevant Application Server. From the perspective of an SGP/ASP, the Routing Context uniquely identifies the range of traffic associated with a

particular Application Server, which the ASP is configured to receive. There is a 1:1 relationship between a Routing Context value and a Routing Key within an AS. Therefore the Routing Context can be viewed as an index into an AS Table containing the AS Routing Keys.

Address Mapping Function (AMF) - The AMF is an implementation dependent function that is responsible for resolving the address presented in the incoming SCCP/SUA message to correct SCTP association for the desired endpoint. The AMF MAY use routing context / rouging key information as selection criteria for the appropriate SCTP association.

Fail-over - The capability to re-route signalling traffic as required to an alternate Application Server Process, or group of ASPs, within an Application Server in the event of failure or unavailability of a currently used Application Server Process. Fail-over may apply upon the return to service of a previously unavailable Application Server Process.

Network Byte Order - Most significant byte first, a.k.a. Big Endian.

Layer Management - Layer Management is a nodal function that handles the inputs and outputs between the SUA layer and a local management entity.

Host - The computing platform that the SGP or ASP process is running on.

Stream - A stream refers to an SCTP stream; a uni-directional logical channel established from one SCTP endpoint to another associated SCTP endpoint, within which all user messages are delivered in-sequence except for those submitted to the un-ordered delivery service.

Transport address - an address that serves as a source or destination for the unreliable packet transport service used by SCTP. In IP networks, a transport address is defined by the combination of an IP address and an SCTP port number. Note, only one SCTP port may be defined for each endpoint, but each SCTP endpoint may have multiple IP addresses.

1.3 Signalling Transport Architecture

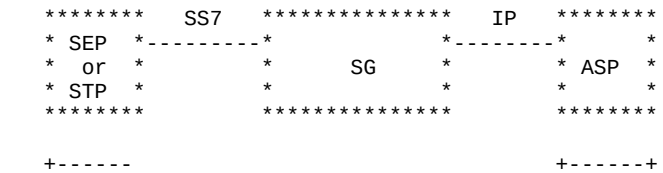
The framework architecture that has been defined for SCN signalling transport over IP [2719] uses multiple components, including an IP transport protocol, a signalling common transport protocol and an adaptation module to support the services expected by a particular SCN signalling protocol from its underlying protocol layer.

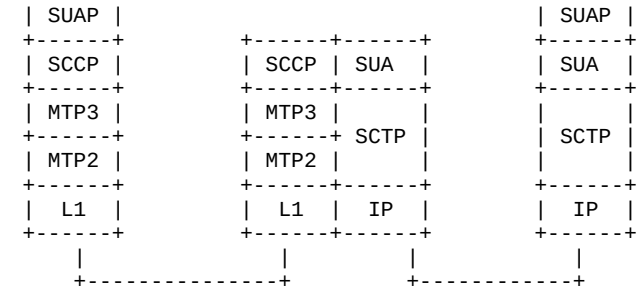
In general terms, the SUA architecture can be modeled as a peer-to-peer architecture. The first section considers the SS7-IP

interworking architectures for connectionless and connection-oriented transport. For this case, it is assumed that the ASP initiates the establishment of the SCTP association with SG.

1.3.1 Protocol Architecture for Connectionless Transport

In this architecture, the SCCP and SUA layers interface in the SG. Interworking between the SCCP and SUA layers is needed to provide for the transfer of the user messages as well as the management messages.





SUAP - SCCP/SUA User Protocol (TCAP, for example)
STP - SS7 Signalling Transfer Point

See Appendix A.3.1 for operation recommendations.

1.3.1.1 SG as endpoint

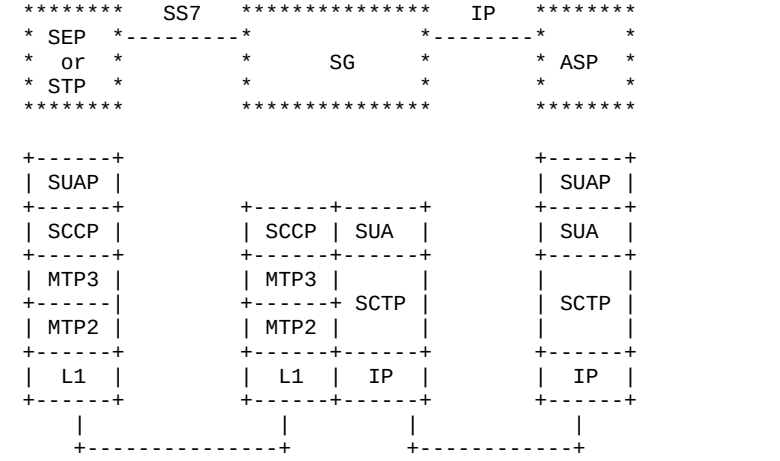
In this case, the connectionless SCCP messages are routed on PC and SSN. The subsystem identified by SSN and Routing Context is regarded as local to the SG. This means from SS7 point of view, the SCCP-user is located at the SG.

1.3.1.2 SG as relay-point

A Global Title translation is executed at the SG, before the destination of the message can be determined. The actual location of the SCCP-user is irrelevant to the SS7 network. GT Translation yields an "SCCP entity", from an AS can be derived. Selection of the AS is thus based on the SCCP called party address (and possibly other SS7 parameters depending on the implementation).

1.3.2 Protocol Architecture for Connection-Oriented Transport

In this architecture, the SCCP and SUA layers interface in the SGP to associate the two connection sections needed for the connection-oriented data transfer between SEP and ASP. Both connection sections are setup when routing the Connect Request messages from SEP via SGP to ASP or the other way. The routing of the Connect Request message is done in the same way as described in 1.3.1.

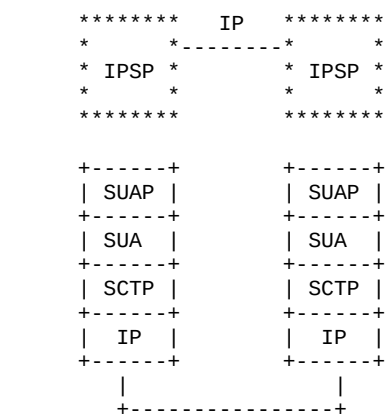


SUAP - SCCP/SUA Application Protocol (e.g. - RANAP/RNSAP)
STP - SS7 Signalling Transfer Point

See Appendix A.3.2 for operation recommendations.

1.3.3 All IP Architecture

This architecture can be used to carry a protocol that uses the transport services of SCCP, but is contained with an IP network. This allows extra flexibility in developing networks, especially when interaction between legacy signalling is not needed. The architecture removes the need for signalling gateway functionality.



SUAP - SCCP/SUA Application Protocol (e.g. - RANAP/RNSAP)

1.3.4 ASP Fail-over Model and Terminology

The SUA protocol supports ASP fail-over functions to support a high availability of transaction processing capability.

An Application Server can be considered as a list of all ASPs configured/registered to handle SCCP-user messages within a certain range of routing information, known as a Routing Key. One or more ASPs in the list may normally be active to handle traffic, while others may be inactive but available in the event of failure or unavailability of the active ASP(s).

For operation recommendations, see Appendix A.

1.4 Services Provided by the SUA Layer

1.4.1 Support for the transport of SCCP-User Messages

The SUA supports the transfer of SCCP-user messages. The SUA layer at the SG and at the ASP support the seamless transport the user messages between the SG and the ASP.

1.4.2 SCCP Protocol Class Support

Depending upon the SCCP-users supported, the SUA shall support the 4 possible SCCP protocol classes transparently. The SCCP protocol classes are defined as follows:

* Protocol class 0 provides unordered transfer of SCCP-user messages in a connectionless manner.

* Protocol class 1 allows the SCCP-user to select the in-sequence delivery of SCCP-user messages in a connectionless manner.

* Protocol class 2 allows the bi-directional transfer of SCCP-user messages by setting up a temporary or permanent signalling connection.

* Protocol class 3 allows the features of protocol class 2 with the inclusion of flow control. Detection of message loss or mis-sequencing is included.

Protocol classes 0 and 1 make up the SCCP connectionless service. Protocol classes 2 and 3 make up the SCCP connection-oriented service.

1.4.3 Native Management Functions

The SUA layer provides the capability to indicate errors associated with the SUA-protocol messages and to provide notification to local management and the remote peer as is necessary.

1.4.4 Interworking with SCCP Network Management Functions

SUA uses the existing ASP management messages for ASP status handling. The interworking with SCCP management messages consists of DUNA, DAVA, DAUD, DRST, DUPU or SCON messages on receipt of SSP, SSA, SST or SSC to the appropriate ASPs. See also chapter 1.4.5. The primitives below are considered to be send between the SCCP and SUA management functions in the SG to trigger events in the IP and SS7 domain.

Generic Name	Specific Name	ANSI/ITU Reference
N-State	Request	ITU-Q.711 Chap 6.3.2.3.2 (Tab 14/Q.711)
	Indication	ANSI-T1.112 Chap 2.3.2.3.2 (Tab 8E/T1.112.1)
N-Pcstate	Indication	ITU-Q.711 Chap 6.3.2.3.3 (Tab 15/Q.711)
		ANSI-T1.112 Chap 2.3.2.3.4 (Tab 8G/T1.112.1)
N-Coord	Request	ITU-Q.711 Chap 6.3.2.3.1 (Tab 13/Q.711)
	Indication	ANSI-T1.112 Chap 2.3.2.3.3 (Tab 8F/T1.112.1)
	Response	
	Confirm	

1.4.5 Support for the management between the SGP and ASP.

The SUA layer should provide interworking with SCCP management functions at the SG for seamless inter-operation between the SCN network and the IP network. It should:

* Provide an indication to the SCCP-user at an ASP that a SS7 endpoint/peer is unreachable.
* Provide an indication to the SCCP-user at an ASP that a SS7 endpoint/peer is reachable.
* Provide congestion indication to SCCP-user at an ASP.
* Provide the initiation of an audit of SS7 endpoints at the SG.

1.4.6 Relay function

For network scalability purposes, the SUA may be enhanced with a relay functionality to determine the next hop SCTP association towards the destination SUA endpoint.

The determination of the next hop may be based on Global Title information (e.g. E.164 number), in analogy with SCCP GTT in SS7 networks, modeled in [ITU-T Q.714]. It may also be based on Hostname information, IP address or pointcode contained in the called party address.

This allows for greater scalability, reliability and flexibility in wide-scale deployments of SUA. The usage of a relay function is a deployment decision.

1.5 Internal Functions Provided in the SUA Layer

To perform its addressing and relaying capabilities, the SUA makes use of an Address Mapping Function (AMF). This function is considered part of SUA, but the way it is realized is left implementation / deployment dependent (local tables, DNS [2916], LDAP, etc.)

The AMF is invoked when a message is received at the incoming interface. The AMF is responsible for resolving the address presented in the incoming SCCP/SUA message to SCTP associations to destinations within the IP network. The AMF will select the appropriate SCTP association based upon routing context / routing key information available. The destination might be the end SUA node or a SUA relay node. The Routing Keys reference an Application Server, which will have one or more ASPs processing traffic for the AS. The availability and status of the ASPs is handled by SUA ASP management messages.

Possible SS7 address/routing information that comprise a Routing Key entry includes, for example, OPC, DPC, SIO found in the MTP3 routing label, SCCP subsystem number, or Transaction ID. IP addresses and hostnames can also be used as Routing Key Information.

It is expected that the routing keys be provisioned via a MIB, dynamic registration or external process, such as a database.

1.5.1 Address Mapping at the SG

Normally, one or more ASPs are active in the AS (i.e., currently processing traffic) but in certain failure and transition cases it is possible that there may not be an active ASP available. The SGP will buffer the message destined for this AS for a time t(r) or until an ASP becomes available. When no ASP becomes available before expiry of t(r), the SGP will flush the buffered messages and initiate the appropriate return or refusal procedures.

If there is no match for an incoming message, a default treatment MAY be specified. Possible solutions are to provide a default Application Server to direct all unallocated traffic to a (set of) default ASP(s), or to drop the messages and provide a notification to management. The treatment of unallocated traffic is implementation dependent.

1.5.2 Address Mapping at the ASP

To direct messages to the SS7 network, the ASP MAY perform an address mapping to choose the proper SGP for a given message. This is accomplished by observing the Destination Point Code and other elements of the outgoing message, SS7 network status, SGP availability, and Routing Context configuration tables.

A Signalling Gateway may be composed of one or more SGPs. There is, however, no SUA messaging to manage the status of an SGP. Whenever an SCTP association to an SGP exists, it is assumed to be available. Also, every SGP of one SG communicating with one ASP regarding one AS provides identical SS7 connectivity to this ASP.

An ASP routes responses to the SGP that it received messages from; within the routing context which it is currently active and receiving traffic. The routing context itself is used by the ASP to select the SGP.

1.5.3 Address Mapping Function at a Relay Node

The relay function is invoked when:

- Routing is on Global Title
- Routing is on Hostname
- Routing is on SSN and PC or SSN and IP Address and the address presented is not the one of the relay node

Translation/resolution of the above address information yields one of the following:

- Route on SSN: SCTP association ID towards the destination node, SSN and optionally Routing Context and/or IP address.
- Route on GT: SCTP association ID towards next relay node, (new) GT and optionally SSN and/or Routing Context.

- Routing on Hostname: SCTP association ID towards next relay node, (new) Hostname and optionally SSN and/or Routing Context.
- A local SUA-user (combined relay/end node)

To prevent looping, an SS7 hop counter is used. The originating end node (be it an SS7 or an IP node) sets the value of the SS7 hop counter to the maximum value (15 or less). Each time the relay function is invoked within an intermediate (relay) node, the SS7 hop counter is decremented. When the value reaches zero, the return or refusal procedures are invoked with reason "Hop counter violation".

1.5.4 SCTP Stream Mapping

The SUA supports SCTP streams. The SG/AS needs to maintain a list of SCTP and SUA-users for mapping purposes. SCCP-users requiring sequenced message transfer need to be sent over a stream supporting sequenced delivery.

SUA uses stream 0 for SUA management messages. It is OPTIONAL that sequenced delivery be used to preserve the order of management message delivery.

Stream selection based on protocol class:

- Protocol class 0: SUA MAY select unordered delivery. The stream selected is based on traffic information available to the SGP or ASP.
- Protocol class 1: SUA MUST select ordered delivery. The stream selected is based upon the sequence parameter given by the upper layer over the primitive interface and other traffic information available to the SGP or ASP
- Protocol classes 2 and 3: SUA MUST select ordered delivery. The stream selected is based upon the source local reference of the connection and other traffic information available to the SGP or ASP.

1.5.5 Flow Control

Local Management at an ASP may wish to stop traffic across an SCTP association to temporarily remove the association from service or to perform testing and maintenance activity. The function could optionally be used to control the start of traffic on to a newly available SCTP association.

1.5.6 Congestion Management

The SUA layer is informed of local and IP network congestion by means of an implementation-dependent function (e.g., an

implementation-dependent indication from the SCTP of IP network congestion).

At an ASP or IPSP, the SUA layer indicates congestion to local SCCP-Users by means of an appropriate SCCP primitive (e.g. N-INFORM, N-NOTICE), as per current SCCP procedures, to invoke appropriate upper layer responses. When an SG determines that the transport of SS7 messages is encountering congestion, the SG MAY trigger SS7 SCCP Congestion messages to originating SS7 nodes, per the congestion procedures of the relevant SCCP standard. The triggering of SS7 SCCP Management messages from an SG is an implementation-dependent function.

The SUA layer at an ASP or IPSP MAY indicate local congestion to an SUA peer with an SCON message. When an SG receives a congestion message (SCON) from an ASP, and the SG determines that an endpoint is now encountering congestion, it MAY trigger congestion procedures of the relevant SCCP standard.

1.6 Definition of SUA Boundaries

1.6.1 Definition of the upper boundary

The following primitives are supported between the SUA and an SCCP-user (a reference to ITU and ANSI sections where these primitives and corresponding parameters are described, is also given):

Generic Name	Specific Name	ANSI/ITU Reference
N-Connect	Request	ITU-Q.711 Chap 6.1.1.2.2 (Tab 2/Q.711)
	Indication	ANSI-T1.112 Chap 2.1.1.2.2 (Tab 2/T1.112.1)
	Response	
	Confirm	
N-Data	Request	ITU-Q.711 Chap 6.1.1.2.3 (Tab 3/Q.711)
	Indication	ANSI-T1.112 Chap 2.1.1.2.3 (Tab 3/T1.112.1)
N-Expedited Data	Request	ITU-Q.711 Chap 6.1.1.2.3 (Tab 4/Q.711)
	Indication	ANSI-T1.112 Chap 2.1.1.2.3 (Tab 4/T1.112.1)
N-Reset	Request	ITU-Q.711 Chap 6.1.1.2.3 (Tab 5/Q.711)
	Indication	ANSI-T1.112 Chap 2.1.1.2.3 (Tab 5/T1.112.1)
	Response	
	Confirm	
N-Disconnect	Request	ITU-Q.711 Chap 6.1.1.2.4 (Tab 6/Q.711)
	Indication	ANSI-T1.112 Chap 2.1.1.2.4 (Tab 6/T1.112.1)
N-Inform	Request	ITU-Q.711 Chap 6.1.1.3.1 (Tab 7/Q.711)
	Indication	ANSI-T1.112 Chap 2.1.1.2.5 (Tab 6A/T1.112.1)
N-Unit Data	Request	ITU-Q.711 Chap 6.2.2.3.1 (Tab 10/Q.711)
	Indication	ANSI-T1.112 Chap 2.2.2.3.1 (Tab 8A/T1.112.1)

N-Notice	Indication	ITU-Q.711 Chap 6.2.2.3.2 (Tab 11/Q.711)
		ANSI-T1.112 Chap 2.2.2.3.2 (Tab 8B/T1.112.1)

1.6.2 Definition of the lower boundary

The upper layer primitives provided by the SCTP are provided in [SCTP].

1.6.3 Definition of the Boundary between SUA and Layer Management

M-SCTP_ESTABLISH request
Direction: LM -> SUA
Purpose: LM requests ASP to establish an SCTP association with its peer.

M-STCP_ESTABLISH confirm
Direction: SUA -> LM
Purpose: ASP confirms to LM that it has established an SCTP association with its peer.

M-SCTP_ESTABLISH indication
Direction: SUA -> LM
Purpose: SUA informs LM that a remote ASP has established an SCTP association.

M-SCTP_RELEASE request
Direction: LM -> SUA
Purpose: LM requests ASP to release an SCTP association with its peer.

M-SCTP_RELEASE confirm
Direction: SUA -> LM
Purpose: ASP confirms to LM that it has released SCTP association with its peer.

M-SCTP_RELEASE indication
Direction: SUA -> LM
Purpose: SUA informs LM that a remote ASP has released an SCTP Association or the SCTP association has failed.

M-SCTP RESTART indication
Direction: SUA -> LM
Purpose: SUA informs LM that an SCTP restart indication has been received.

M-SCTP_STATUS request
Direction: LM -> SUA
Purpose: LM requests SUA to report the status of an SCTP association.

M-SCTP_STATUS confirm
Direction: SUA -> LM

Purpose: SUA responds with the status of an SCTP association.

M-SCTP STATUS indication
Direction: SUA -> LM
Purpose: SUA reports the status of an SCTP association.

M-ASP_STATUS request
Direction: LM -> SUA
Purpose: LM requests SUA to report the status of a local or remote ASP.

M-ASP_STATUS confirm
Direction: SUA -> LM
Purpose: SUA reports status of local or remote ASP.

M-AS_STATUS request
Direction: LM -> SUA
Purpose: LM requests SUA to report the status of an AS.

M-AS_STATUS confirm
Direction: SUA -> LM
Purpose: SUA reports the status of an AS.

M-NOTIFY indication
Direction: SUA -> LM
Purpose: SUA reports that it has received a Notify message from its

peer.

M-ERROR indication
Direction: SUA -> LM
Purpose: SUA reports that it has received an Error message from its peer or that a local operation has been unsuccessful.

M-ASP_UP request
Direction: LM -> SUA
Purpose: LM requests ASP to start its operation and send an ASP Up message to its peer.

M-ASP_UP confirm
Direction: SUA -> LM
Purpose: ASP reports that is has received an ASP UP Ack message from its peer.

M-ASP_UP indication
Direction: SUA -> LM
Purpose: SUA reports it has successfully processed an incoming ASP Up message from its peer.

M-ASP_DOWN request
Direction: LM -> SUA
Purpose: LM requests ASP to stop its operation and send an ASP Down message to its peer.

M-ASP_DOWN confirm
Direction: SUA -> LM
Purpose: ASP reports that is has received an ASP Down Ack message from its peer.

M-ASP_DOWN indication
Direction: SUA -> LM
Purpose: SUA reports it has successfully processed an incoming ASP Down message from its peer, or the SCTP association has been lost/reset.

M-ASP_ACTIVE request
Direction: LM -> SUA
Purpose: LM requests ASP to send an ASP Active message to its peer.

M-ASP_ACTIVE confirm
Direction: SUA -> LM
Purpose: ASP reports that is has received an ASP Active Ack message from its peer.

M-ASP_ACTIVE indication
Direction: SUA -> LM
Purpose: SUA reports it has successfully processed an incoming ASP Active message from its peer.

M-ASP_INACTIVE request
Direction: LM -> SUA
Purpose: LM requests ASP to send an ASP Inactive message to its peer.

M-ASP_INACTIVE confirm
Direction: LM -> SUA
Purpose: ASP reports that is has received an ASP Inactive Ack message from its peer.

M-ASP_INACTIVE indication
Direction: SUA -> LM
Purpose: SUA reports it has successfully processed an incoming ASP Inactive message from its peer.

M-AS_ACTIVE indication
Direction: SUA -> LM
Purpose: SUA reports that an AS has moved to the AS-ACTIVE state.

M-AS_INACTIVE indication
Direction: SUA -> LM
Purpose: SUA reports that an AS has moved to the AS-INACTIVE state.

M-AS_DOWN indication
Direction: SUA -> LM
Purpose: SUA reports that an AS has moved to the AS-DOWN state.

If dynamic registration of RK is supported by the SUA layer, the layer MAY support the following additional primitives:

M-RK_REG request
Direction: LM -> SUA
Purpose: LM requests ASP to register RK(s) with its peer by sending REG REQ message

M-RK_REG confirm
Direction: SUA -> LM
Purpose: ASP reports that it has received REG RSP message with registration status as successful from its peer.

M-RK_REG indication
Direction: SUA -> LM
Purpose: SUA informs LM that it has successfully processed an incoming REG REQ message.

M-RK_DEREG request
Direction: LM -> SUA
Purpose: LM requests ASP to deregister RK(s) with its peer by sending DEREG REQ message.

M-RK_DEREG confirm
Direction: SUA -> LM
Purpose: ASP reports that it has received DEREG RESP message with deregistration status as successful from its peer.

M-RK_DEREG indication
Direction: SUA -> LM
Purpose: SUA informs LM that it has successfully processed an incoming DEREG REQ from its peer.

2 Conventions

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, NOT RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

3 Protocol Elements

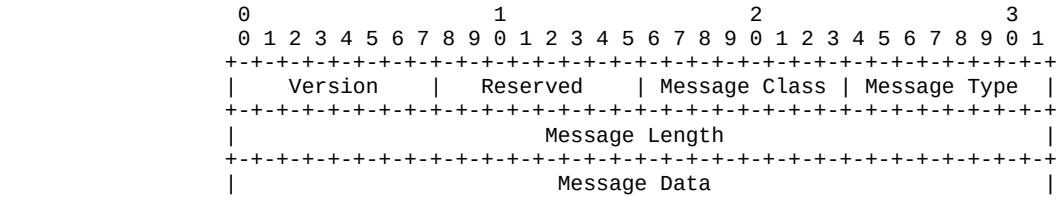
The general message format includes a Common Message Header together with a list of zero or more parameters as defined by the Message Type.

For forward compatibility, all Message Types may have attached parameters even if none are specified in this version.

3.1 Common Message Header

The protocol messages for the SCCP-User Adaptation Protocol requires a message structure which contains a version, message class, message type, message length and message contents. This message header is

common among all signalling protocol adaptation layers:



Note that the 'data' portion of SUA messages SHALL contain SCCP-User data, not the encapsulated SCCP message.

Optional parameters can only occur at most once in an SUA message.

3.1.1 SUA Protocol Version

The version field (ver) contains the version of the SUA adaptation layer. The supported versions are:

1	SUA version 1.0

3.1.2 Message Classes

Message Classes

0	SUA Management (MGMT) Message
1	Reserved
2	Signalling Network Management (SNM) Messages
3	ASP State Maintenance (ASPSM) Messages
4	ASP Traffic Maintenance (ASPTM) Messages
5	Reserved
6	Reserved
7	Connectionless Messages
8	Connection-Oriented Messages
9	Routing Key Management (RKM) Messages.
10 - 127	Reserved by the IETF
128 - 255	Reserved for IETF-Defined Message Class Extensions

3.1.3 Message Types

SUA Management Messages

0	Error (ERR)
1	Notify (NTFY)
2 - 127	Reserved by the IETF
128- 255	Reserved for IETF-Defined Message Class Extensions

Signalling Network Management (SNM) Messages

0	Reserved
1	Destination Unavailable (DUNA)
2	Destination Available (DAVA)
3	Destination State Audit (DAUD)
4	Network Congestion (SCON)
5	Destination User Part Unavailable (DUPU)
6	Destination Restricted (DRST)
7 - 127	Reserved by the IETF
128 - 255	Reserved for IETF-Defined Message Class Extensions

Application Server Process State Maintenance (ASPSM) Messages

0	Reserved
1	ASP Up (UP)
2	ASP Down (DOWN)
3	Heartbeat (BEAT)
4	ASP Up Ack (UP ACK)
5	ASP Down Ack (DOWN ACK)
6	Heartbeat Ack (BEAT ACK)

```
  7 - 127   Reserved by the IETF
  128 - 255 Reserved for IETF-Defined Message Class Extensions

ASP Traffic Maintenance (ASPTM) Messages

  0         Reserved
  1         ASP Active (ACTIVE)
  2         ASP Inactive (INACTIVE)
  3         ASP Active Ack (ACTIVE ACK)
  4         ASP Inactive Ack (INACTIVE ACK)
  5 - 127   Reserved by the IETF
  128 - 255 Reserved for IETF-Defined Message Class Extensions

Routing Key Management (RKM) Messages

  0         Reserved
  1         Registration Request (REG REQ)
  2         Registration Response (REG RSP)
  3         Deregistration Request (DEREG REQ)
  4         Deregistration Response (DEREG RSP)
  5 - 127   Reserved by the IETF
  128 - 255 Reserved for IETF-Defined Message Class Extensions

Connectionless (CL) Messages

  0         Reserved
  1         Connectionless Data Transfer (CLDT)
  2         Connectionless Data Response (CLDR)
  3 - 127   Reserved by the IETF
  128 - 255 Reserved for IETF-Defined Message Class Extensions
```



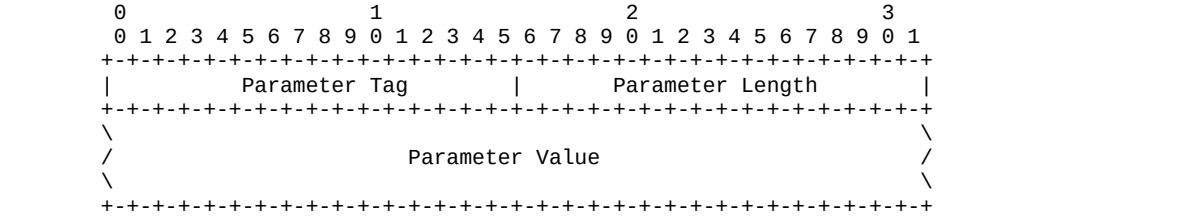
```
Connection-Oriented (CO) Messages

  0         Reserved
  1         Connection Request (CORE)
  2         Connection Acknowledge (COAK)
  3         Connection Refused (COREF)
  4         Release Request (RELRE)
  5         Release Complete (RELCO)
  6         Reset Confirm (RESCO)
  7         Reset Request (RESRE)
  8         Connection Oriented Data Transfer (CODT)
  9         Connection Oriented Data Acknowledge (CODA)
  10        Connection Oriented Error (COERR)
  11        Inactivity Test (COIT)
  12 - 127  Reserved by the IETF
  128 - 255 Reserved for IETF-Defined Message Class Extensions
```

3.1.4 Message Length

The Message Length defines the length of the message in octets, including the header and including all padding bytes. Message Length is a 32-bit identifier.

3.1.5 Tag-Length-Value Format

SUA messages consist of a Common Header followed by zero or more parameters, as defined by the message type. The Tag-Length-Value (TLV) parameters contained in a message are defined in a Tag-Length-Value format as shown below.



Parameter Tag: 16 bits (unsigned integer)

Tag field is a 16-bit identifier of the type of parameter. It takes a value of 0 to 65535.

Parameter Length: 16 bits (unsigned integer)

The Parameter Length field contains the size of the parameter in bytes, including the Parameter Tag, Parameter Length, and Parameter Value fields. The Parameter Length does not include any padding bytes. However, composite parameters will contain all

padding bytes, since all parameters contained within this composite parameter will be considered multiples of 4 bytes.

Parameter Value: variable-length.

The Parameter Value field contains the actual information to be trasnfered in the parameter.

The total length of a parameter (including Tag, Parameter Length and Value fields) MUST be a multiple of 4 bytes. If the length of the parameter is not a multiple of 4 bytes, the sender pads the parameter at the end (i.e., after the Parameter Value field) with all zero bytes. The length of the padding is NOT included in the parameter length field. A sender should NEVER pad with more than 3 bytes. The receiver MUST ignore the padding bytes.

Implementation note: the use of TLV in principle allows the parameters to be placed in a random order in the message. However, some guidelines should be considered for easy processing in the following order:

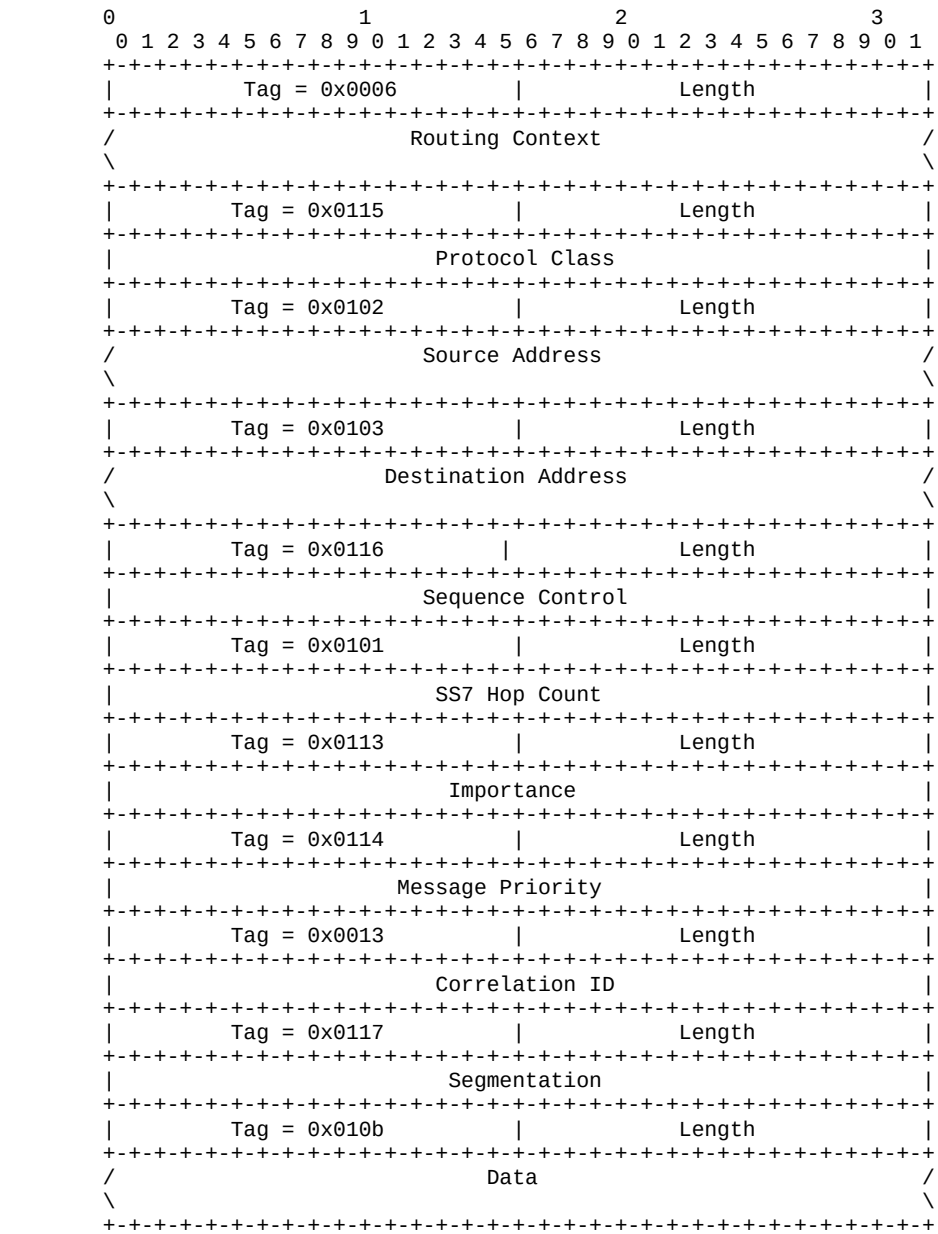
- Parameters needed to correctly process other message parameters, preferably should precede these parameters (such as Routing Context).
- Mandatory parameters preferably SHOULD precede any optional parameters.
- The data parameter will normally be the final one in the message.
- The receiver SHOULD accept parameters in any order, except where explicitly mandated.

3.2 SUA Connectionless Messages

The following section describes the SUA Connectionless transfer messages and parameter contents. The general message format includes a Common Message Header together with a list of zero or more parameters as defined by the Message Type. All Message Types can have attached parameters.

3.2.1 Connectionless Data Transfer (CLDT)

This message transfers data between one SUA to another.

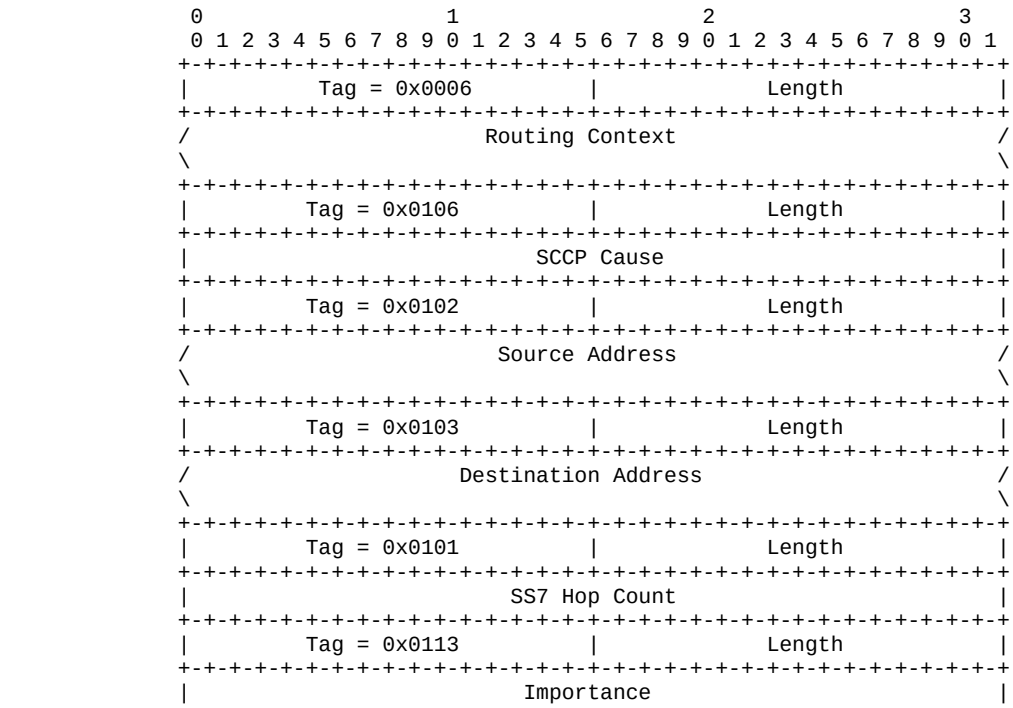


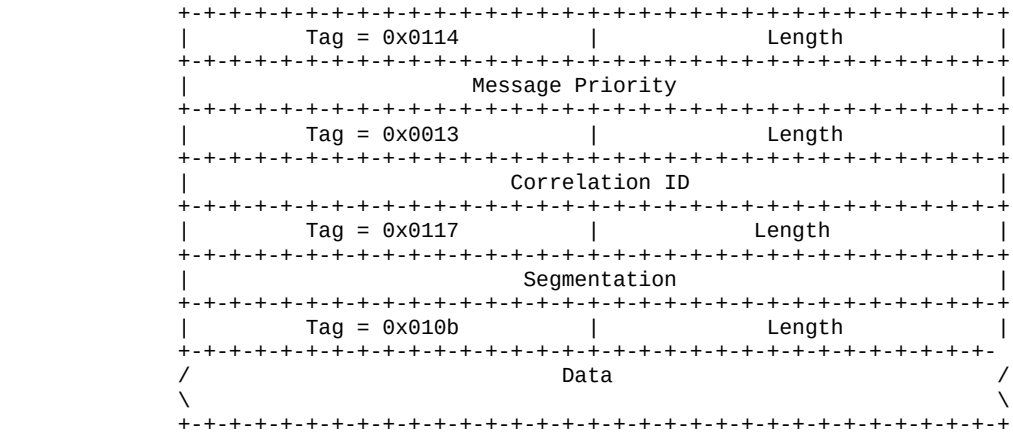
Parameters	
Routing Context	Mandatory
Protocol Class	Mandatory
Source Address	Mandatory
Destination Address	Mandatory
Sequence Control	Mandatory
SS7 Hop Count	Optional
Importance	Optional
Message Priority	Optional
Correlation ID	Optional
Segmentation	Optional
Data	Mandatory

Implementation note: This message covers the following SCCP messages: unitdata (UDT), extended unitdata (XUDT), long unitdata (LUDT).

3.2.2 Connectionless Data Response (CLDR)

This message is used as a response message by the peer to report errors in the received CLDT message, when the return on error option is set.





Parameters

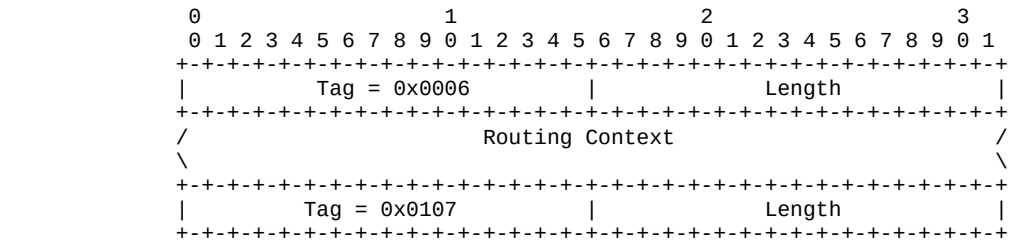
Routing Context	Mandatory
SCCP Cause	Mandatory
Source Address	Mandatory
Destination Address	Mandatory
SS7 Hop Count	Optional
Importance	Optional
Message Priority	Optional
Correlation ID	Optional
Segmentation	Optional
Data	Optional

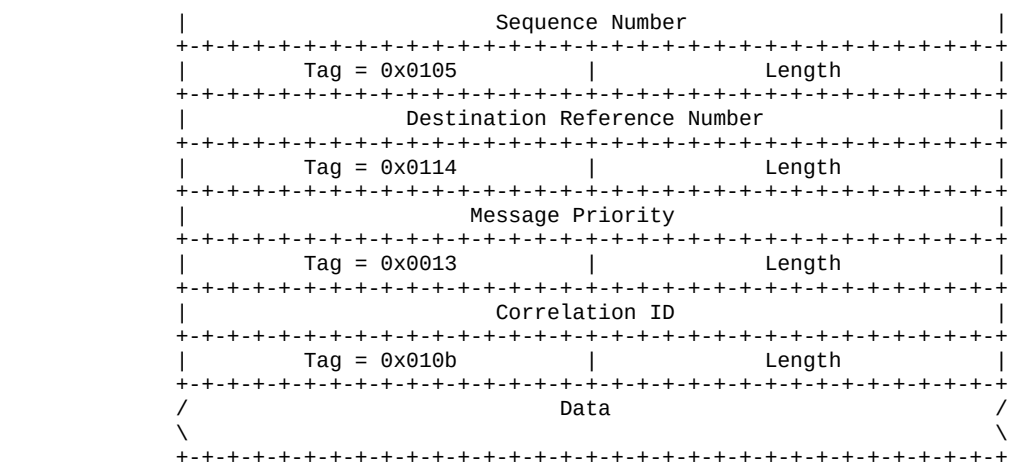
Implementation note: This message covers the following SCCP messages: unitdata service (UDTS), extended unitdata service (XUDTS) and long unitdata service (LUDTS).

3.3 Connection Oriented Messages

3.3.1 Connection Oriented Data Transfer (CODT)

This message transfers data between one SUA to another for connection-oriented service.





Parameters

Routing Context	Mandatory
Sequence Number	Optional *1
Destination Reference Number	Mandatory
Message Priority	Optional
Correlation ID	Optional
Data	Mandatory

NOTE *1: This parameter is not present in case of Expedited Data (ED).

Implementation note: In order for the CODT to represent DT1, DT2 and ED messages, the following conditions MUST be met:

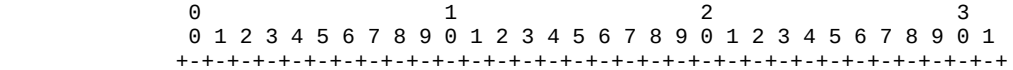
DT1 is represented by a CODT when:
Sequence Number parameter is present (contains "more" indicator).

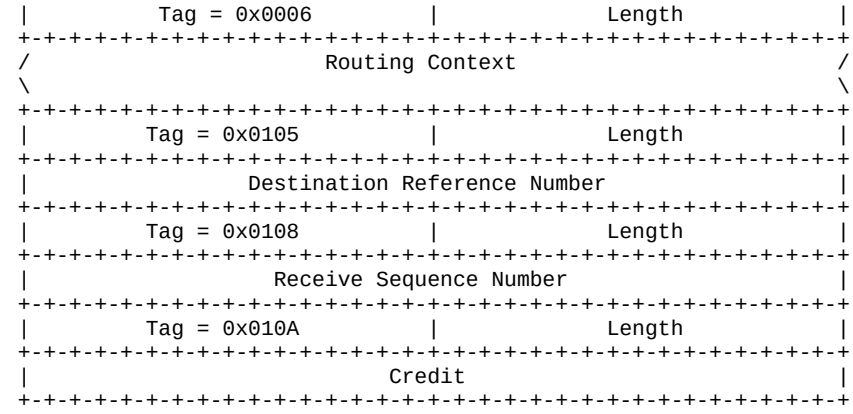
DT2 is represented by a CODT when:
Sequence Number parameter is present (contains P(S), P(R) and more indicator)

ED is represented by a CODT with:
Sequence Number parameter is not present

3.3.2 Connection Oriented Data Acknowledge (CODA)

This message is used to acknowledge receipt of data by the peer. This message is used only with protocol class 3.





Parameters

Routing Context	Mandatory
Destination Reference Number	Mandatory
Receive Sequence Number	Optional *1
Credit	Mandatory *1

NOTE *1: Mandatory when representing Data Acknowledgement (AK).

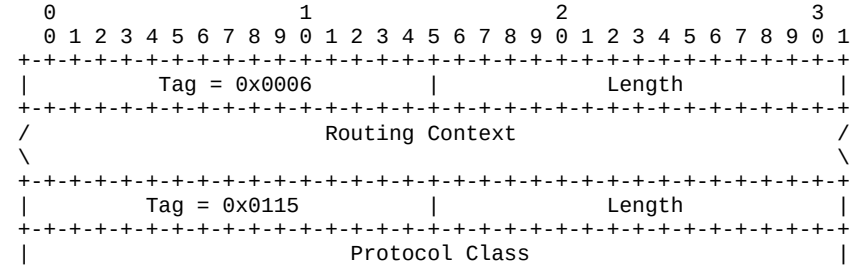
Implementation note: In order for the CODA to represent DA and EA messages, the following conditions MUST be met:

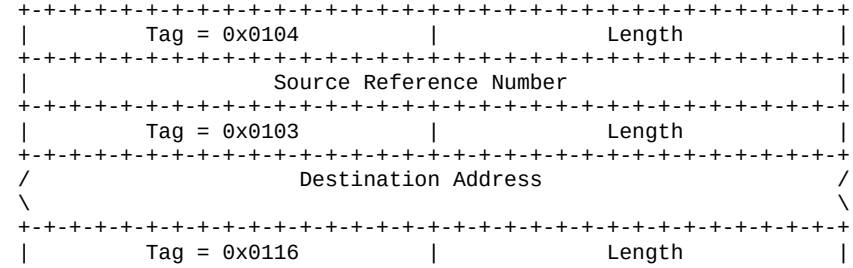
DA is represented by a CODA when:
Receive Sequence Number parameter is present (contains P(S), P(R) and more indicator)

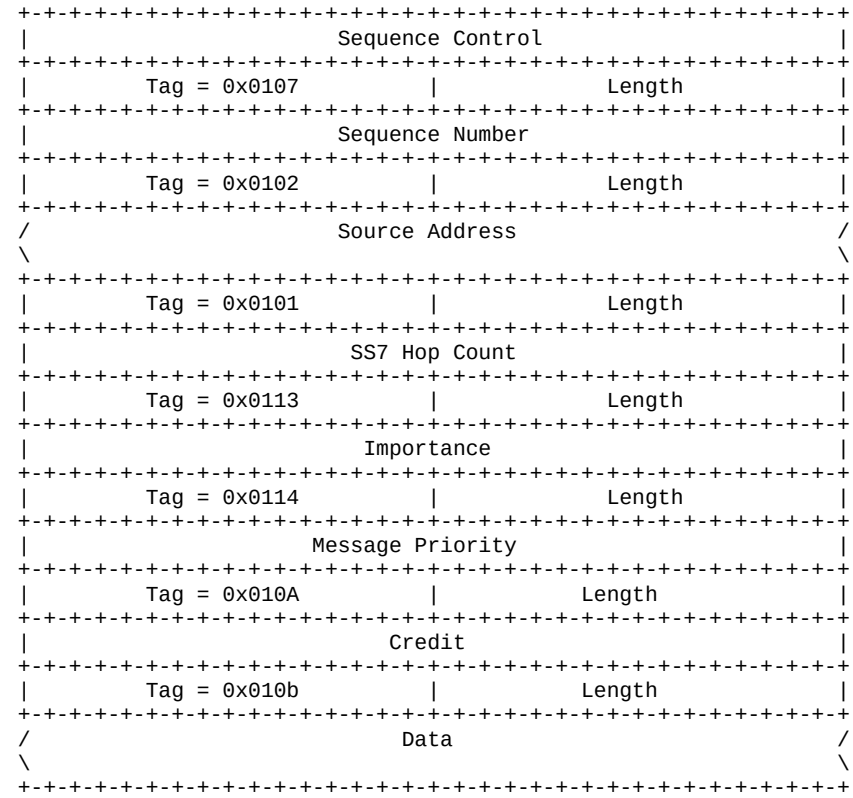
EA is represented by a CODA when:
Receive Sequence Number parameter is not present

3.3.3 Connection Request (CORE)

This message is used for establishing a signalling connection between two peer endpoints.







Parameters	
Routing Context	Mandatory
Protocol Class	Mandatory
Source Reference Number	Mandatory
Destination Address	Mandatory
Sequence Control	Mandatory
Sequence Number	Optional *1

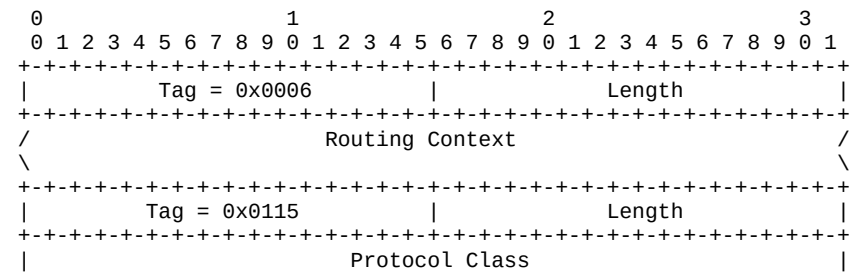
Source Address	Optional
SS7 Hop Count	Optional
Importance	Optional
Message Priority	Optional
Credit	Optional *1
Data	Optional

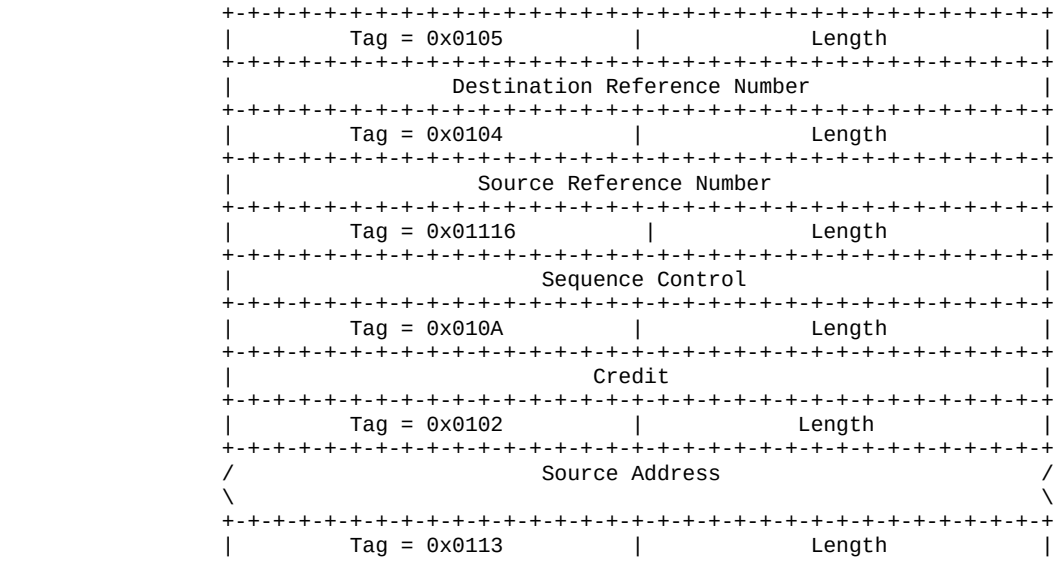
NOTE *1: Manditory for protocol class 3 only.

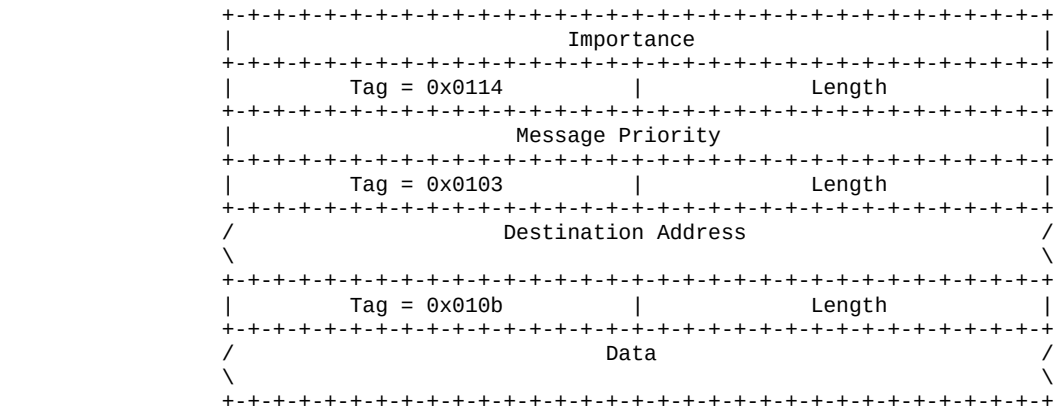
Implementation note: This message covers the following SCCP message: Connection Request (CR).

3.3.4 Connection Acknowledge (COAK)

This message is used to acknowledge a connection request from the peer endpoint.







Parameters	
Routing Context	Mandatory
Protocol Class	Mandatory
Destination Reference Number	Mandatory
Source Reference Number	Mandatory
Sequence Control	Mandatory
Credit	Mandatory *2
Source Address	Optional
Importance	Optional
Message Priority	Optional
Destination Address	Optional *1
Data	Optional

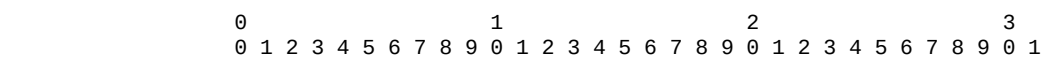
NOTE *1: Destination Address parameter will be present in case that the received CORE message conveys the Source Address parameter.

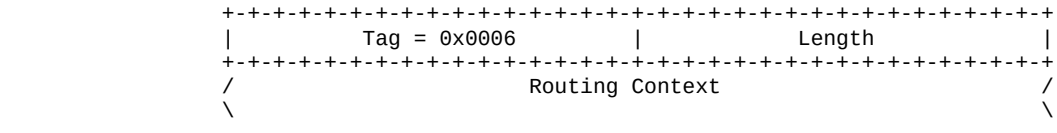
NOTE *2: Only applicable for protocol class 3.

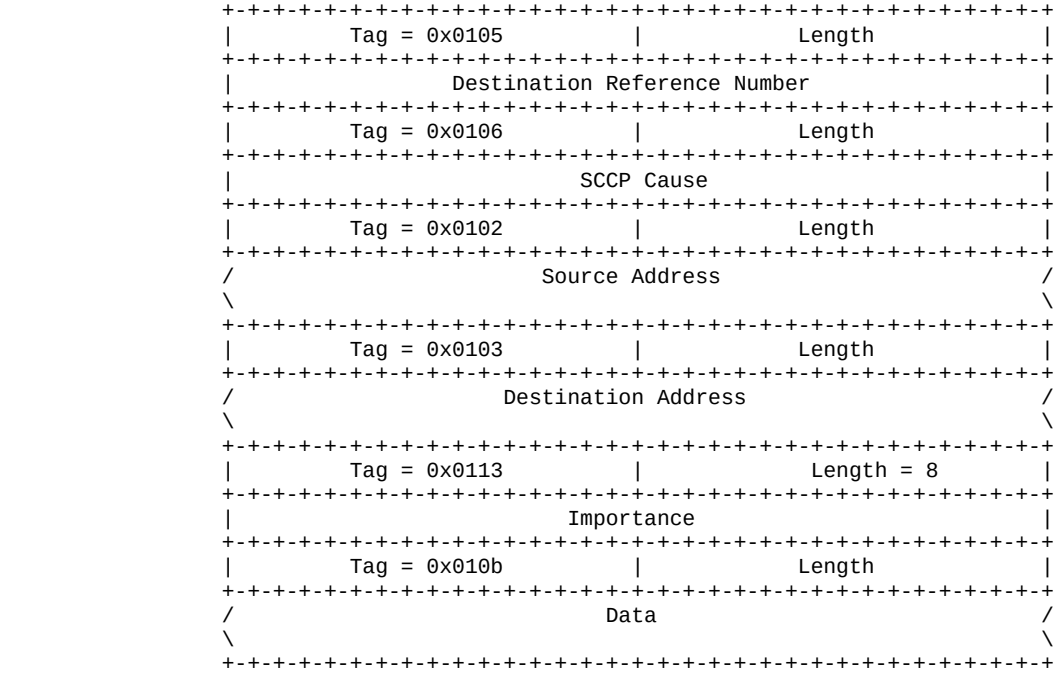
Implementation note: This message covers the following SCCP message: Connection Confirm (CC).

3.3.5 Connection Refused (COREF)

This message is used to refuse a connection request between two peer endpoints.







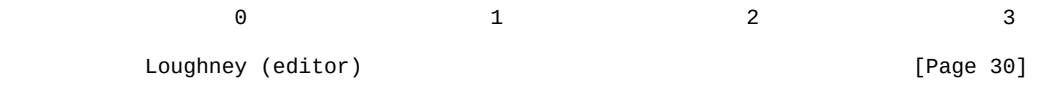
Parameters	
Routing Context	Mandatory
Destination Reference Number	Mandatory
SCCP Cause	Mandatory
Source Address	Optional
Destination Address	Optional *1
Importance	Optional
Data	Optional

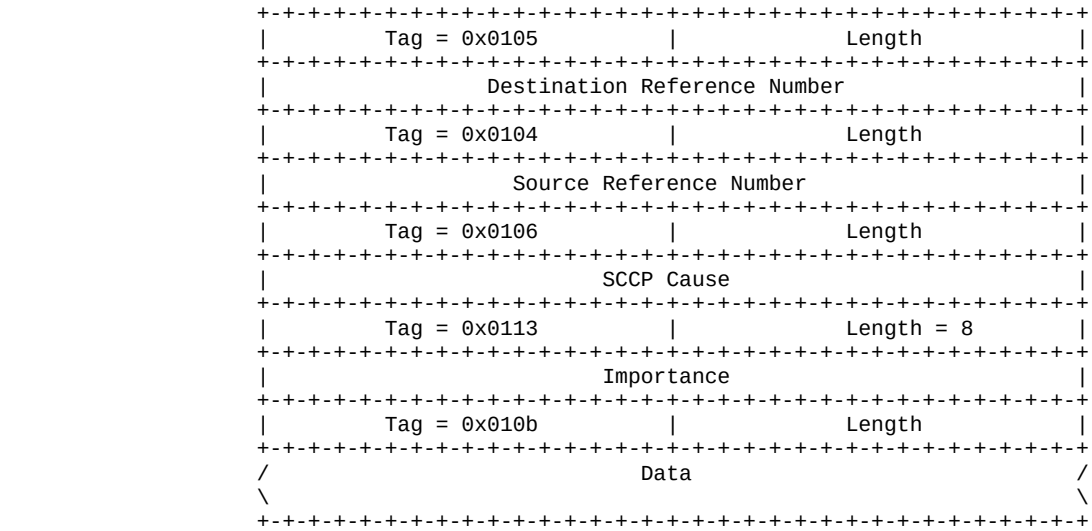
Note *1: Destination Address parameter will be present in case that the received CORE message conveys the Source Address parameter.

Implementation note: This message covers the following SCCP message: Connection REFused (CREF).

3.3.6 Release Request (RELRE)

This message is used to request a signalling connection between two peer endpoints be released. All associated resources can then be released.



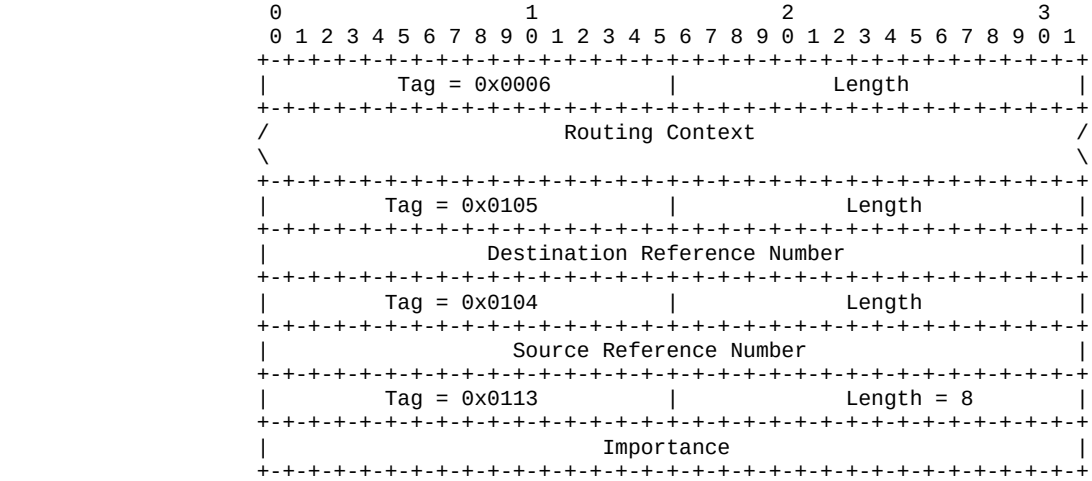


Parameters	
Routing Context	Mandatory
Destination Reference Number	Mandatory
Source Reference Number	Mandatory
SCCP Cause	Mandatory
Importance	Optional
Data	Optional

Implementation note: This message covers the following SCCP message: connection ReLeaSeD (RLSD).

3.3.7 Release Complete (RELCO)

This message is used to acknowledge the release of a signalling connection between two peer endpoints. All associated resources should be released.



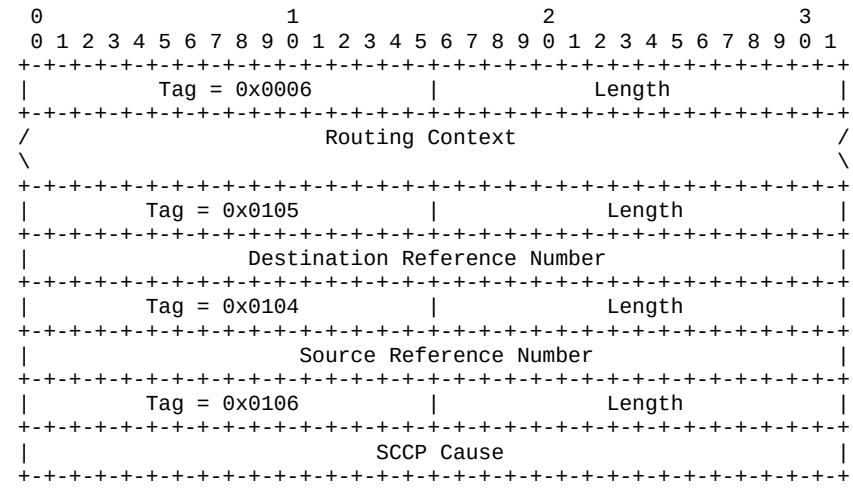
Parameters	
Routing Context	Mandatory
Destination Reference Number	Mandatory

Source Reference Number	Mandatory
Importance	Optional

Implementation note: This message covers the following SCCP message: ReLease Complete (RLC).

3.3.8 Reset Request (RESRE)

This message is used to indicate that the sending SCCP/SUA wants to initiate a reset procedure (re-initialization of sequence numbers) to the peer endpoint.



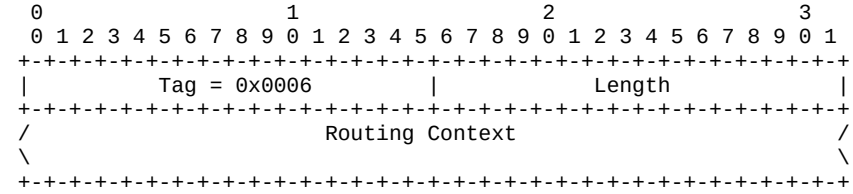
Parameters

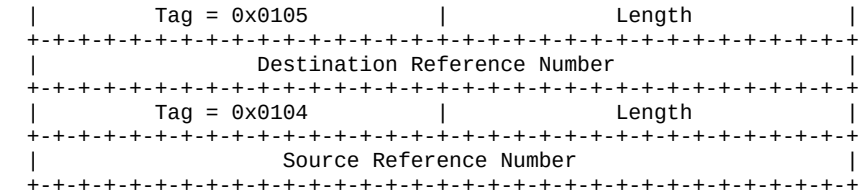
Routing Context	Mandatory
Destination Reference Number	Mandatory
Source Reference Number	Mandatory
SCCP Cause	Mandatory

Implementation note: This message covers the following SCCP message: ReSet Request (RSR).

3.3.9 Reset Confirm (RESCO)

This message is used to confirm the Reset Request.





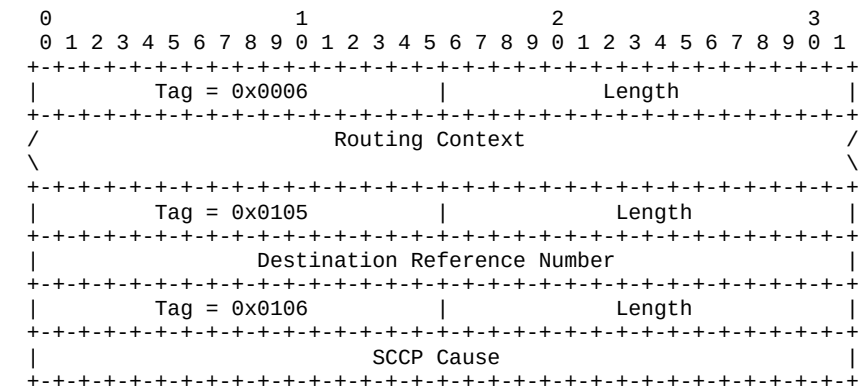
Parameters

Routing Context	Mandatory
Destination Reference Number	Mandatory
Source Reference Number	Mandatory

Implementation note: This message covers the following SCCP message: ReSet Confirmation (RSC).

3.3.10 Connection Oriented Error (COERR)

The COERR message is sent to indicate a protocol data unit error.



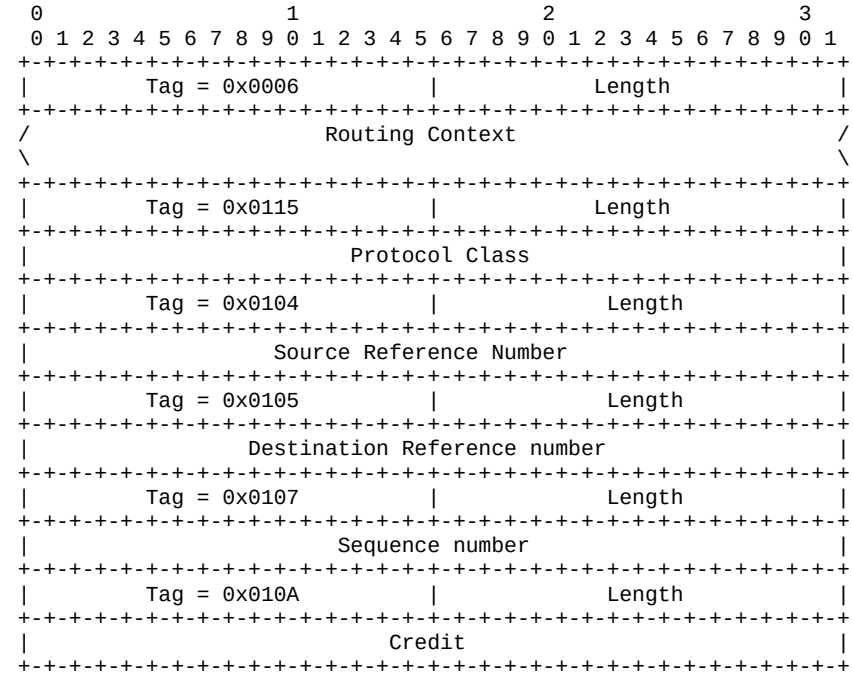
Parameters

Routing Context	Mandatory
Destination Reference Number	Mandatory
SCCP Cause	Mandatory

Implementation note: This message covers the following SCCP message: Protocol Data Unit ERRor (ERR).

3.3.11 Connection Oriented Inactivity Test (COIT)

This message is used for auditing the signalling connection state and the consistency of connection data at both ends of the signalling connection.



Parameters	
Routing Context	Mandatory
Protocol Class	Mandatory
Source Reference Number	Mandatory
Destination Reference number	Mandatory
Sequence Number	Mandatory *1
Credit	Mandatory *1

NOTE *1: Information in these parameter fields reflects those values sent in the last data form 2 or data acknowledgement message. They are ignored if the protocol class indicates class 2.

Implementation note: This message covers the following SCCP message: Inactivity Test (IT).

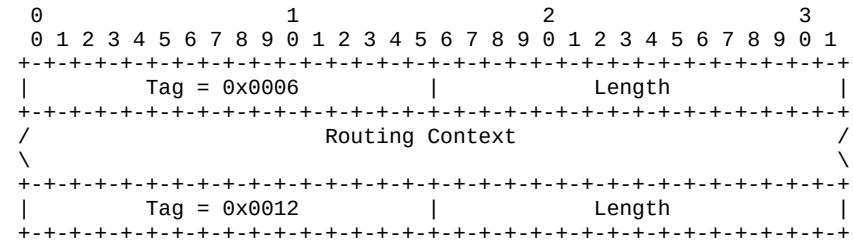
3.4 Signalling Network Management (SNM) Messages

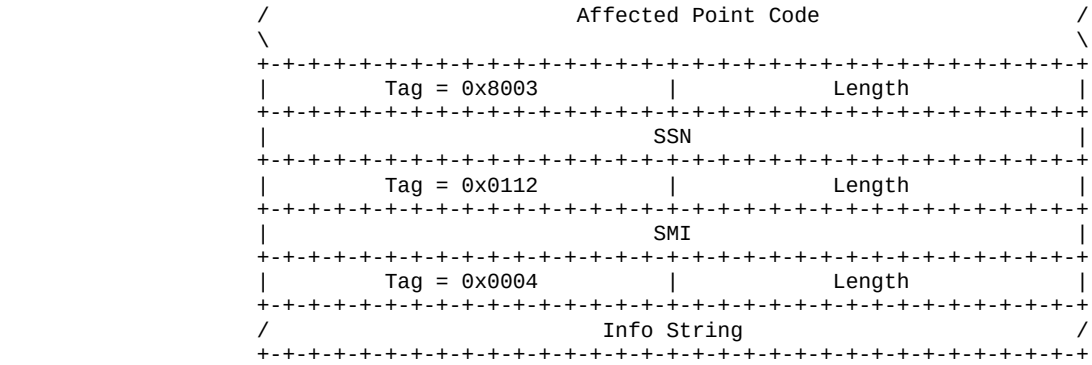
3.4.1 Destination Unavailable (DUNA)

In the scope of SUA, this message is covered by the PC- or N-state indication passed between SCCP and local SCCP-user. The DUNA message

is sent from the SG or relay node to all concerned ASPs (servicing SCCP-users considered local to the SG or relay node, see chapter 1.3.1.1), when a destination or SCCP-user has become unreachable. The SUA-User at the ASP is expected to stop traffic to the affected destination or SCCP-user through the SG or relay node initiating the DUNA.

The format for DUNA Message parameters is as follows:





Parameters

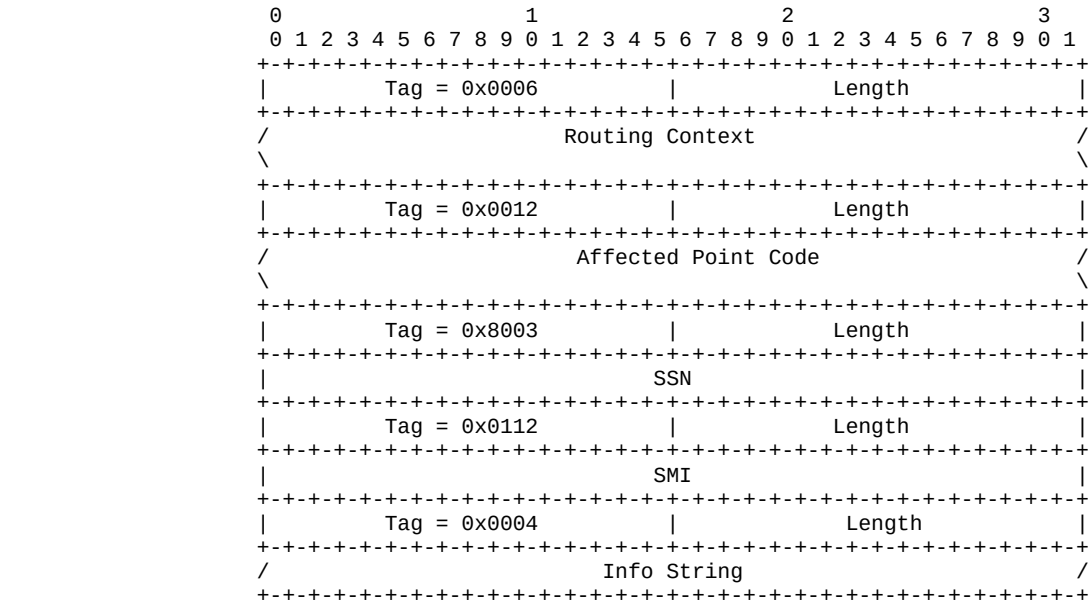
Routing Context	Optional
Affected Point Code	Mandatory *1
SSN	Optional *1
SMI	Optional
Info String	Optional

Note 1: When the SSN is included, the DUNA message corresponds to the SCCP N-STATE primitive. When SSN is not, the DUNA message corresponds to the SCCP N-PCSTATE primitive.

3.4.2 Destination Available (DAVA)

In the scope of SUA, this message is covered by the PC- and N-state indication passed between SCCP and local SCCP-user. The DAVA message is sent from the SG or relay node to all concerned ASPs (servicing

SCCP-users considered local to the SG or relay node, see chapter 1.3.1.1) to indicate that a destination (PC or SCCP-user) is now reachable. The ASP SUA-User protocol is expected to resume traffic to the affected destination through the SG or relay node initiating the DAVA.



Parameters

Routing Context	Optional
Affected Point Code	Mandatory *1
SSN	Optional *1
SMI	Optional

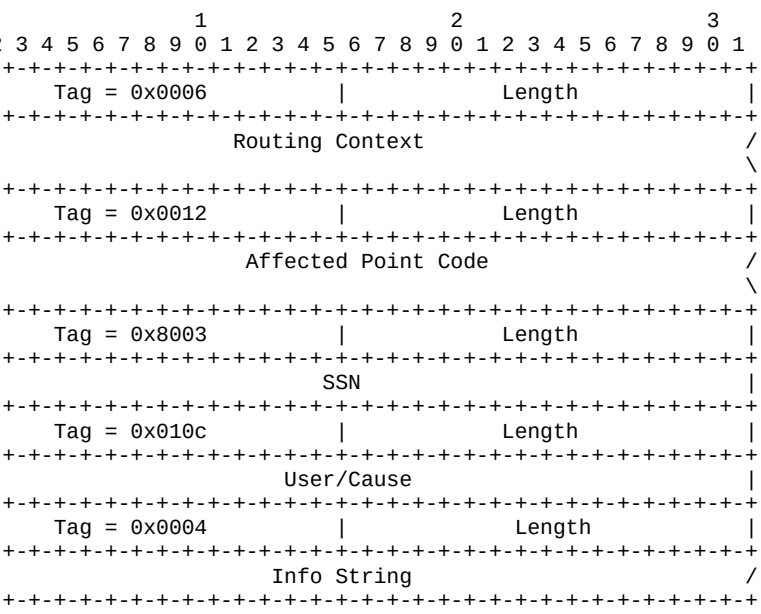
Info String	Optional

Note 1: When the SSN is included, the DAVA message corresponds to the SCCP N-STATE primitive. When SSN is not included, the DAVA message corresponds to the SCCP N-PCSTATE primitive. The Affected Point Code can only contain one point code when SSN is present.

3.4.3 Destination State Audit (DAUD)

The DAUD message can be sent from the ASP to the SG (or relay node) to query the availability state of the routes to an affected destination. A DAUD may be sent periodically after the ASP has

received a DUNA, until a DAVA is received. The DAUD can also be sent when an ASP recovers from isolation from the SG (or relay node).



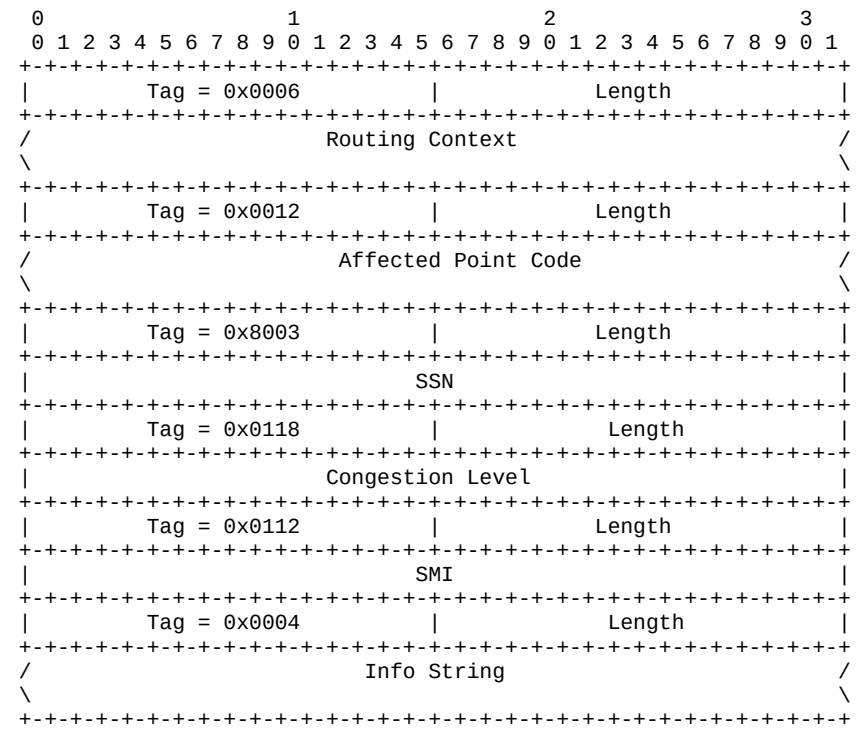
Parameters

Routing Context	Optional
Affected Point Code	Mandatory *1
SSN	Optional *1
User / Cause	Optional
Info String	Optional

Note 1: If the SSN is present, the DAUD is "soliciting" N-STATE primitives, otherwise it is "soliciting" N-PCSTATE primitives.

3.4.4 Network Congestion (SCON)

The SCON message can be sent from the SG or relay node to all concerned ASPs to indicate that the congestion level in the SS7 network to a specified destination has changed.



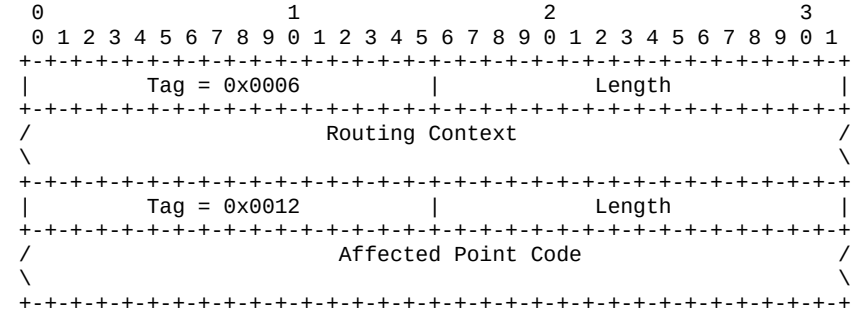
Parameters	
Routing Context	Optional
Affected Point Code	Mandatory *1
SSN	Optional *1
Congestion Level	Mandatory
SMI	Optional
Info String	Optional

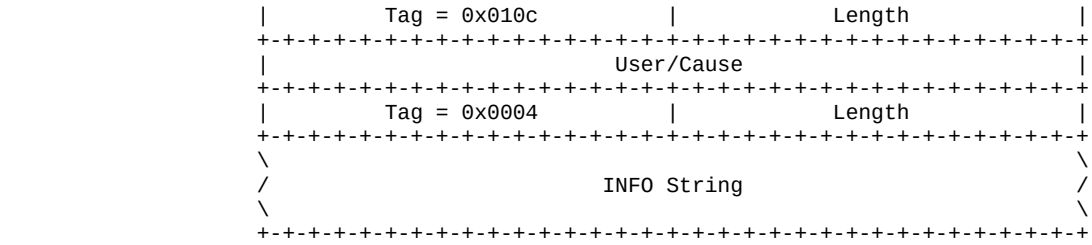
Note 1: When the SSN is included, the SCON message corresponds to the SCCP N-STATE primitive. When SSN is not included, the SCON message corresponds to the SCCP N-PCSTATE primitive.

3.4.5 Destination User Part Unavailable (DUPU)

The DUPU message is used by an SG to inform an ASP that a remote peer at an SS7 node is unavailable.

The format for DUPU message parameters is as follows:





Parameters

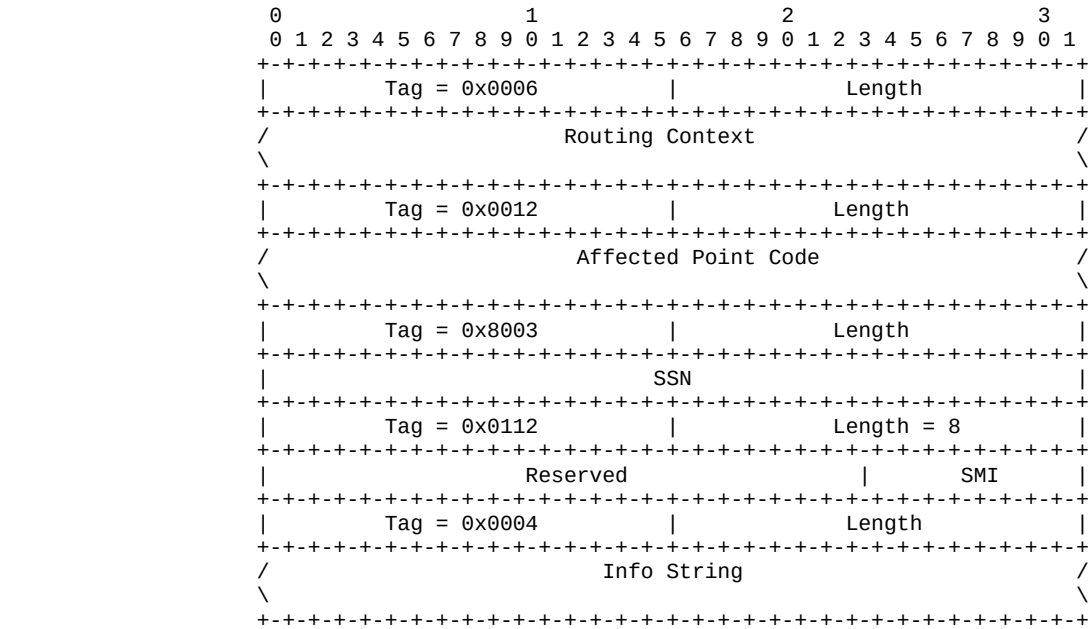
Routing Context	Optional
Affected Point Code	Mandatory *1
User/Cause	Mandatory
Info String	Optional

Note 1: The DUPU corresponds to the SCCP N-PCSTATE primitive.

3.4.6 Destination Restricted (DRST)

The DRST message is optionally sent from the SG to all concerned ASPs to indicate that the SG has determined that one or more destinations are now restricted from the point of view of the SG, or in response to a DAUD message if appropriate. The SUA layer at the ASP is expected to send traffic to the affected destination via an alternate SG of equal priority, but only if such an alternate route exists and is available. If the affected destination is currently considered unavailable by the ASP, the peer should be informed that traffic to the affected destination can be resumed. In this case, the SUA layer should route the traffic through the SG initiating the DRST message.

This message is optional for the SG to send and it is optional for the ASP to act on any information received in the message.



Parameters

Routing Context	Optional
Affected Point Code	Mandatory *1
SSN	Optional *1

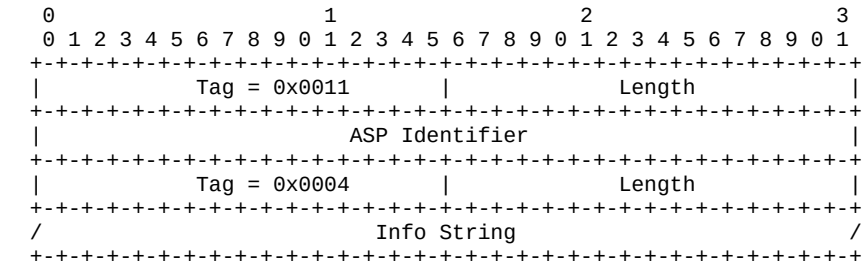
SMI	Optional *1
Info String	Optional

Note 1: The Affected Point Code referes to the node to which become restricted or which has requested coordinated service outgage. When SSN is included in the message parameter, the DRST message corresponds to the SCCP N-COORD primitive. If the SMI parameter is also included in the message, the DRST message corresponds to the N-COORD Request and N-COORD Indication primitives, otherwise, the DRST message corresponse to the N-COORD Response and N-COORD Confirm primitives. The Affected Point Code can only contain one point code when SSN is present. When SSN is not present, DRST corresponds to N-PCSTATE primitive.

3.5 Application Server Process State Maintenance Messages

3.5.1 ASP Up (UP)

The ASP UP (UP) message is used to indicate to a remote SUA peer that the Adaptation layer is up and running.



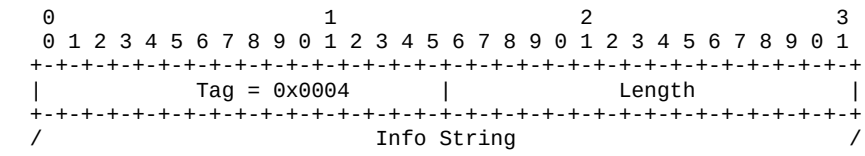
Parameters

ASP Identifier	Optional *1
Info String	Optional

Note 1: ASP Identifier MUST be used where the IPSP/SGP cannot identify the ASP by pre-configured address/port number information (e.g., where an ASP is resident on a Host using dynamic address/port number assignment).

3.5.2 ASP Up Ack (UP ACK)

The ASP UP Ack message is used to acknowledge an ASP-Up message received from a remote SUA peer.

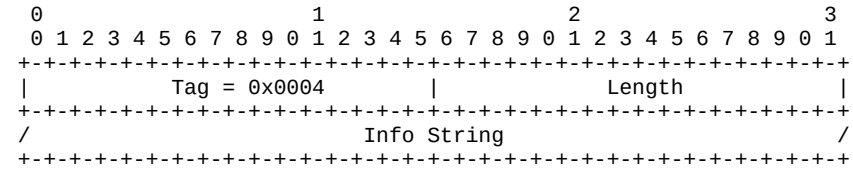


Parameters

Info String	Optional

3.5.3 ASP Down (DOWN)

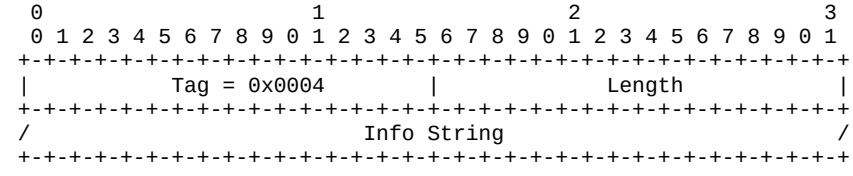
The ASP Down (DOWN) message is used to indicate to a remote SUA peer that the adaptation layer is not running.



Parameters
Info String Optional

3.5.4 ASP Down Ack (DOWN ACK)

The ASP DOWN Ack message is used to acknowledge an ASP-Down message received from a remote SUA peer.



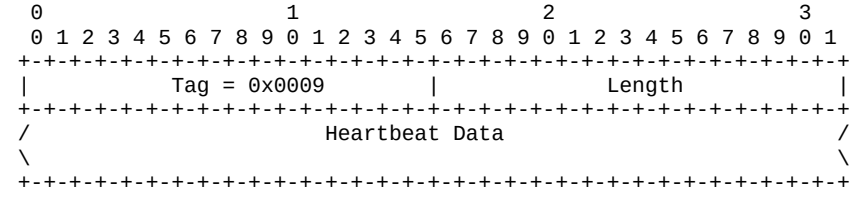
Parameters
Info String Optional

Note: ASP DOWN ACK will always be sent to acknowledge an ASP DOWN.

3.5.5 Heartbeat (BEAT)

The Heartbeat message is optionally used to ensure that the SUA peers are still available to each other.

The format for the BEAT message is as follows:

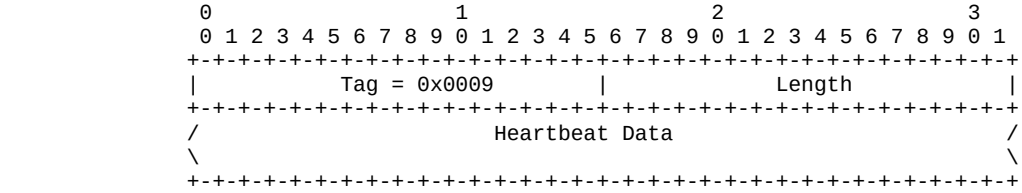


Parameters
Heartbeat Data Optional

3.5.6 Heartbeat Ack (BEAT ACK)

The Heartbeat ACK message is sent in response to a BEAT message. A peer MUST send a BEAT ACK in response to a BEAT message. It includes all the parameters of the received Heartbeat message, without any change.

The format for the BEAT ACK message is as follows:



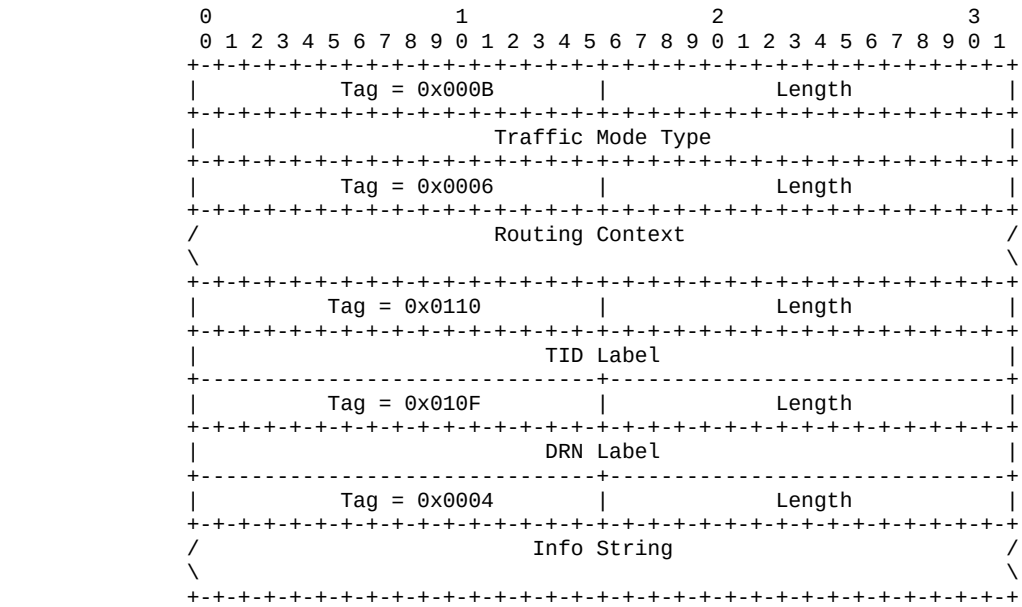
Parameters
Heartbeat Data Optional

3.6 ASP Traffic Maintenance Messages

3.6.1 ASP Active (ACTIVE)

The ASPAC message is sent by an ASP to indicate to a remote SUA peer that it is Active and ready to process signalling traffic for a particular Application Server.

The format for the ACTIVE message is as follows:



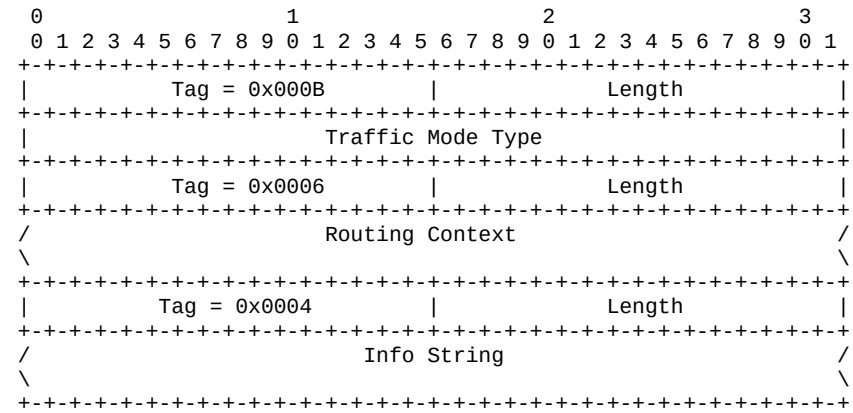
Parameters

Traffic Mode Type	Optional
Routing Context	Optional
TID Label	Optional
DRN Label	Optional
Info String	Optional

3.6.2 ASP Active Ack (ACTIVE ACK)

The ASPAC Ack message is used to acknowledge an ASP-Active message received from a remote SUA peer.

The format for the ACTIVE Ack message is as follows:



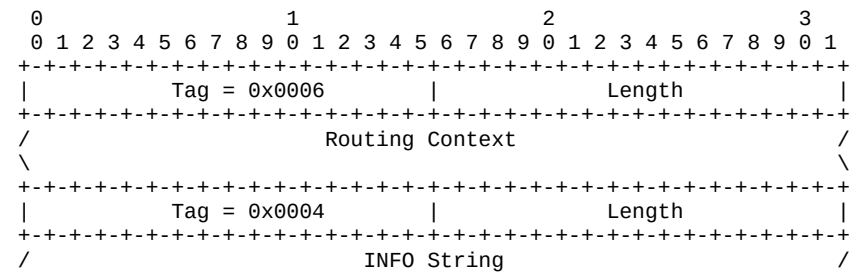
Parameters

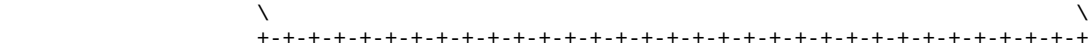
Traffic Mode Type	Optional
Routing Context	Optional
Info String	Optional

3.6.3 ASP Inactive (INACTIVE)

The INACTIVE message is sent by an ASP to indicate to a remote SUA peer that it is no longer processing signalling traffic within a particular Application Server.

The format for the ASPIA message parameters is as follows:





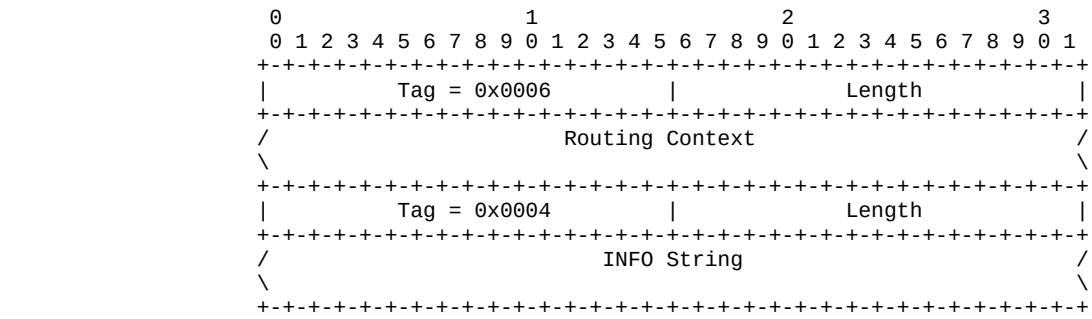
Parameters

Routing Context	Optional
INFO String	Optional

3.6.4 ASP Inactive Ack (INACTIVE ACK)

The INACTIVE Ack message is used to acknowledge an ASP-Inactive message received from a remote SUA peer.

The format for the INACTIVE Ack message is as follows:



Parameters

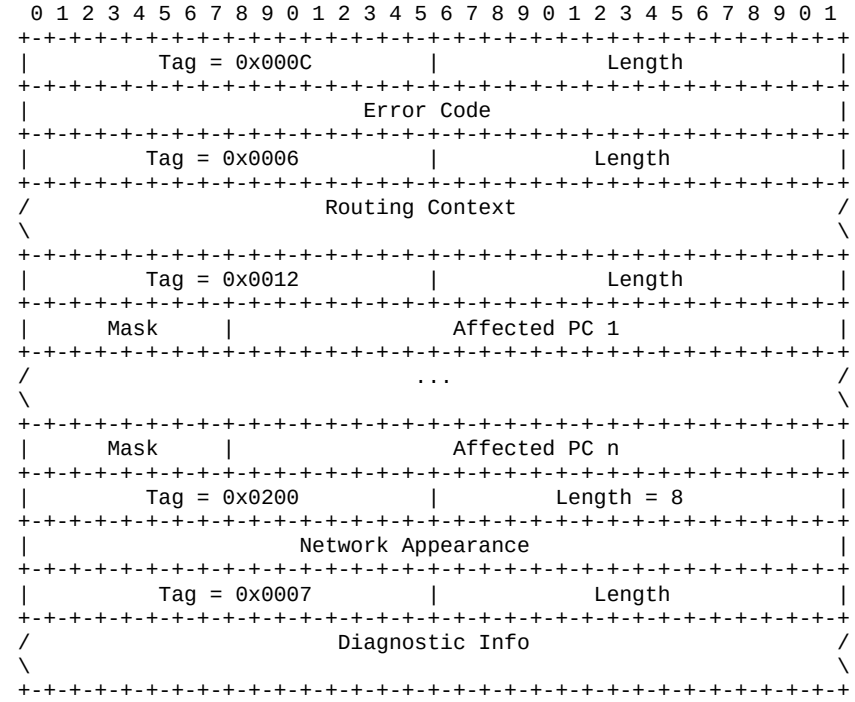
Routing Context	Optional
INFO String	Optional

3.7 SUA Management Messages

These messages are used for managing SUA and the representations of the SCCP subsystems in the SUA layer.

3.7.1 Error (ERR)

The ERR message is sent between two SUA peers to indicate an error situation. The Data parameter is optional, possibly used for error logging and/or debugging.

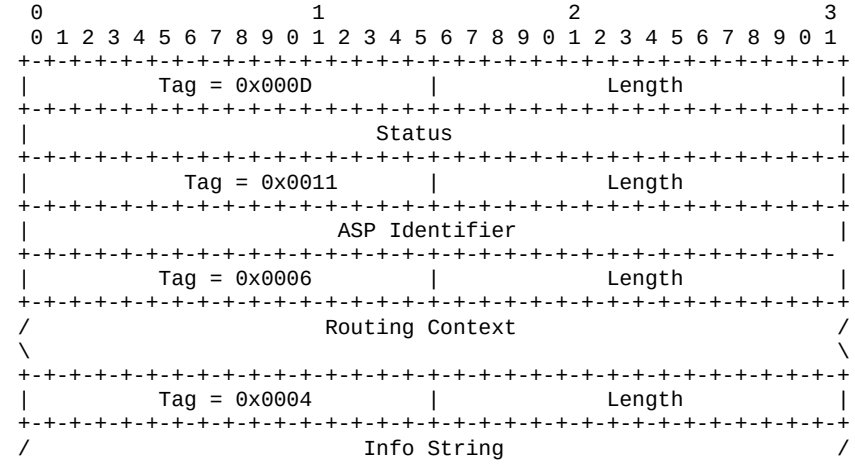


Parameters	
Error Code	Mandatory
Routing Context	Mandatory *1
Network Appearance	Mandatory *1
Affected Point Code	Mandatory *1
Diagnostic Information	Optional

Note 1: Only mandatory for specific error codes.

3.7.2 Notify (NTFY)

The Notify message used to provide an autonomous indication of SUA events to an SUA peer.



The NTFY message contains the following parameters:

Parameters	
Status	Mandatory
ASP Identifier	Optional *1
Routing Context	Optional
Info String	Optional

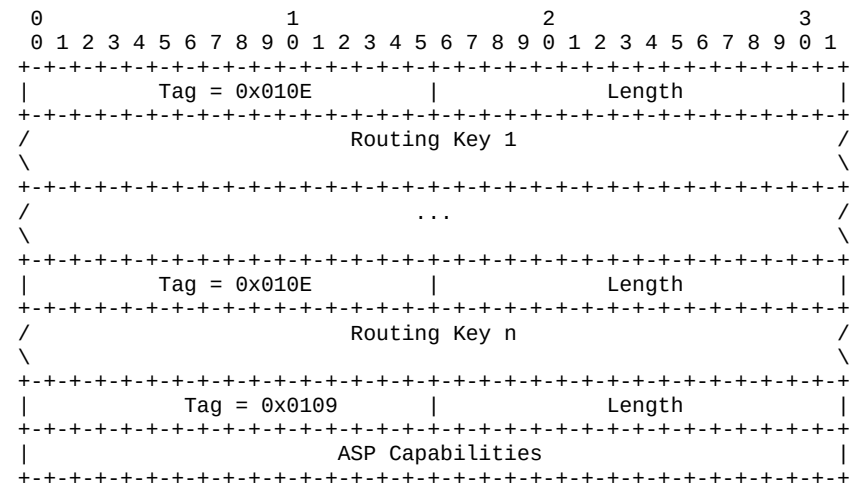
Note 1: ASP Identifier MUST be used where the IPSP/SGP cannot identify the ASP by pre-configured address/port number information (e.g., where an ASP is resident on a Host using dynamic address/port number assignment).

3.8 Routing Key Management (RKM) Messages

3.8.1 Registration Request (REG REQ)

The REG REQ message is sent by an ASP to indicate to a remote SUA peer that it wishes to register one or more given Routing Keys with the remote peer. Typically, an ASP would send this message to an SGP, and expects to receive a REG RSP message in return with an associated Routing Context value.

The format for the REG REQ message is as follows:



The REG REQ message contains the following parameters:

Parameters	
Routing Key	Mandatory *1
ASP Capabilities	Optional

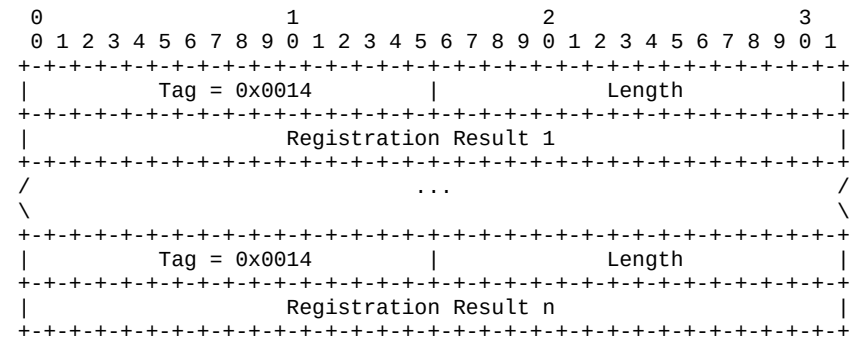
Note 1: One or more Routing Key parameters MAY be included in a single REG REQ message.

3.8.2 Registration Response (REG RSP)

The REG RSP message is sent by an SG to an ASP indicate the result of a previous REG REQ from an ASP. It contains indications of success/failure for registration requests and returns a unique Routing Context value for successful registration requests, to be

used in subsequent SUA Traffic Management protocol messages.

The format for the REG RSP message is as follows:



The REG RSP message contains the following parameters:

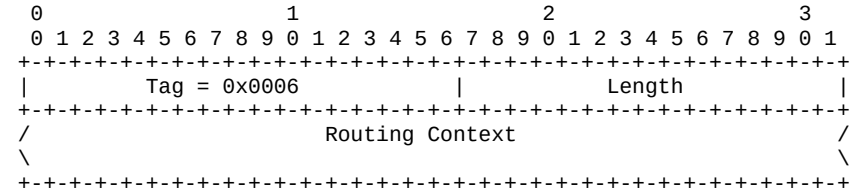
Parameters
Registration Result Mandatory *1

Note 1: One or more Registration Result parameters MAY be included in a single REG RSP message. The number of results in a single REG RSP message can be anywhere from one to the total number of Routing Key parameters found in the corresponding REG REQ message.

3.8.3 Deregistration Request (DEREG REQ)

The DEREG REQ message is sent by an ASP to indicate to a remote SUA peer that it wishes to deregister a given Routing Key. Typically, an ASP would send this message to an SGP, and expects to receive a DEREG RSP message in return with the associated Routing Context value.

The format for the DEREG REQ message is as follows:



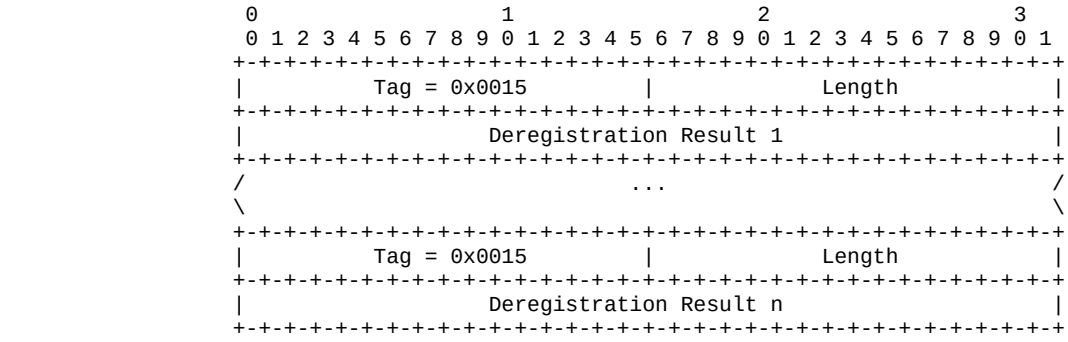
The DEREG REQ message contains the following parameters:

Parameters
Routing Context Mandatory

3.8.4 Deregistration Response (DEREG RSP)

The DEREG RSP message is used as a response to the DEREG REQ message from a remote SUA peer.

The format for the DEREG RSP message is as follows:



The DEREG RSP message contains the following parameters:

Parameters
Deregistration Result Mandatory *1

Note 1: One or more Deregistration Result parameters MAY be included in one DEREG RSP message. The number of results in a single DEREG RSP message can be anywhere from one to the total number of number of Routing Context parameters found in the corresponding DEREG REQ message.

3.9 Common Parameters

These TLV parameters are common across the different adaptation layers.

Parameter Name	Parameter ID
Reserved	0x0000
Not used in SUA	0x0001
Not used in SUA	0x0002
Not used in SUA	0x0003
Info String	0x0004
Not used in SUA	0x0005
Routing Context	0x0006
Diagnostic Info	0x0007
Not used in SUA	0x0008
Heartbeat Data	0x0009
Not Used in SUA	0x000A
Traffic Mode Type	0x000B

Error Code	0x000C
Status	0x000D
Not used in SUA	0x000E
Not used in SUA	0x000F
Not used in SUA	0x0010
ASP Identifier	0x0011
Affected Point Code	0x0012
Correlation ID	0x0013
Registration Result	0x0014
Deregistration Result	0x0015
Registration Status	0x0016
Deregistration Status	0x0017
Local Routing Key Identifier	0x0018

3.9.1 Not Used

Use of Parameter ID 0x0001 in SUA messages is not supported.

3.9.2 Not Used

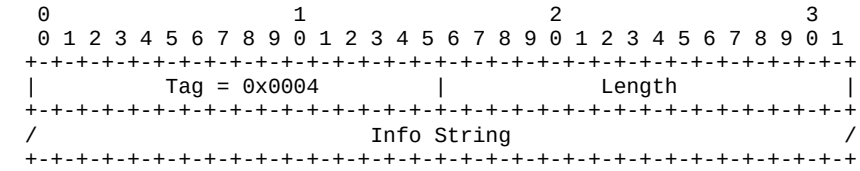
Use of Parameter ID 0x0002 in SUA messages is not supported.

3.9.3 Not Used

Use of Parameter ID 0x0002 in SUA messages is not supported.

3.9.4 Info String

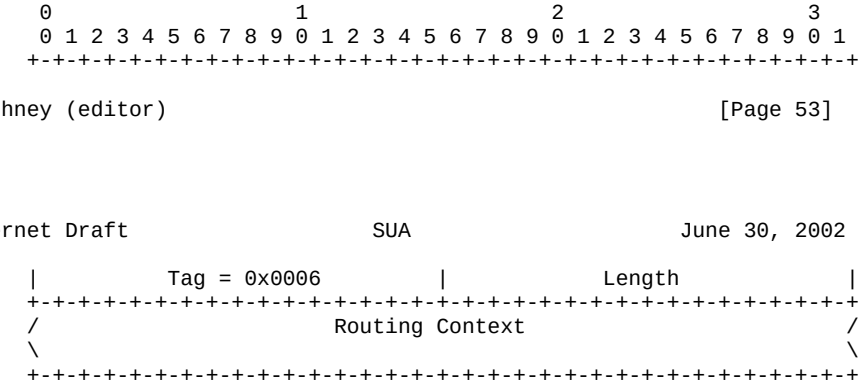
The optional INFO String parameter can carry any meaningful UTF-8 [2279] character string along with the message. Length of the INFO String parameter is from 0 to 255 octets. No procedures are presently identified for its use but service providers may use the INFO String for debugging purposes.



3.9.5 Not Used in SUA

Use of Parameter ID 0x0005 in SUA messages is not supported.

3.9.6 Routing Context



The Routing Context parameter contains (a list of) 4-byte unsigned integers indexing the Application Server traffic that the sending ASP is configured/registered to receive. There is a one-to-one relationship between an index entry and a Routing Key or AS Name.

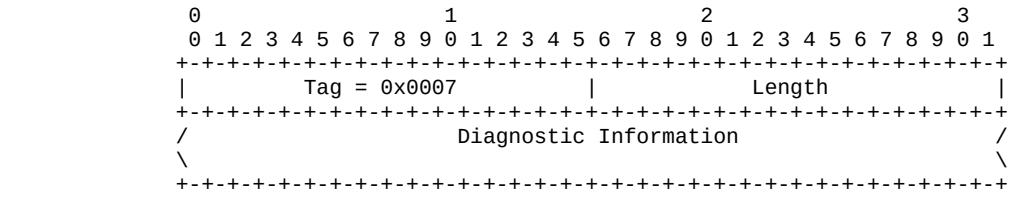
An Application Server Process may be configured to process traffic for more than one logical Application Server. From the perspective of an ASP, a Routing Context defines a range of signalling traffic that the ASP is currently configured to receive from the SG.

Additionally, the Routing Context parameter identifies the SS7 network context for the message, for the purposes of logically separating the signalling traffic between the SGP and the Application Server Process over a common SCTP Association, when needed. An example is where an SGP is logically partitioned to appear as an element in several different national SS7 networks. It implicitly defines the SS7 Point Code format used, the SS7 Network Indicator value and SCCP protocol type/variant/version used within a separate SS7 network. It also defines the network context for the PC and SSN values. Where an SGP operates in the context of a single SS7 network, or individual SCTP associations are dedicated to each SS7 network context, this functionality is not needed.

If the Routing Context parameter is present, it SHOULD be the first parameter in the message as it defines the format and/or interpretation of the parameters containing a PC or SSN value.

3.9.7 Diagnostic Information

The Diagnostic Information can be used to convey any information relevant to an error condition, to assist in the identification of the error condition. In the case of an Adaptation Layer Identifier or Traffic Handling Mode, the Diagnostic Information includes the received parameter. In the other cases, the Diagnostic information may be the first 40 bytes of the offending message.



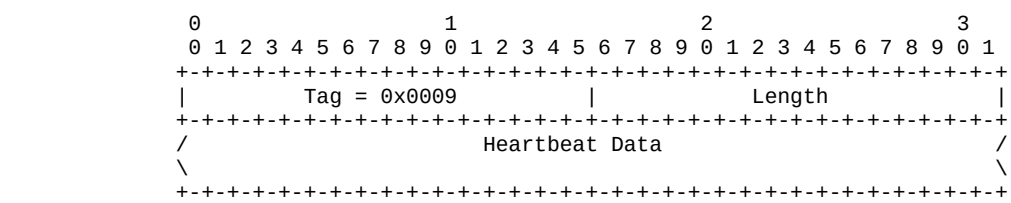
3.9.8 Not Used

Parameter ID 0x0008 is not used in SUA.

3.9.9 Heartbeat Data

The sending node defines the Heartbeat Data field contents. It may include a Heartbeat Sequence Number and/or Timestamp, or other implementation specific details.

The receiver of a Heartbeat message does not process this field as it is only of significance to the sender. The receiver echoes the content of the Heartbeat Data in a BEAT-Ack message.



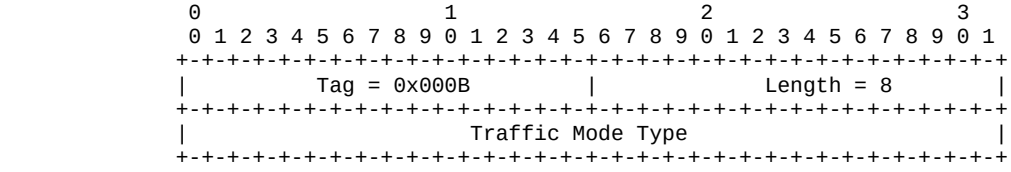
The data field can be used to store information in the heartbeat message useful to the sending node (e.g. the data field can contain a time stamp, a sequence number, etc.).

3.9.10 Not Used

Parameter ID 0x000A is not used in SUA.

3.9.11 Traffic Mode Type

The Traffic Mode Type parameter identifies the traffic mode of operation of the ASP within an AS.



The valid values for Type are shown in the following table.

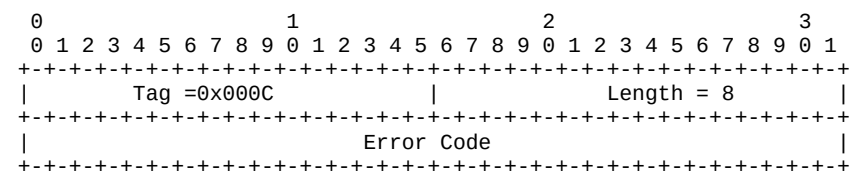
1	Over-ride
2	Load-share
3	Broadcast

Within a Routing Context, Over-ride, Loadshare Types and Broadcast

cannot be mixed. The Over-ride value indicates that the ASP is

operating in Over-ride mode, and the ASP wishes to take over all traffic for an Application Server (i.e., primary/back-up operation), over-riding any currently active ASP in the AS. In Load-share mode, the ASP wishes to share in the traffic distribution with any other currently active ASPs. In Broadcast mode, the ASP wishes to receive the same traffic as any other currently active APSs. When there are insufficient ASPs, the sender may immediately move the ASP to Active.

3.9.12 Error Code



The Error Code parameter indicates the reason for the Error Message. The Error parameter value can be one of the following values:

0x01	Invalid Version
0x02	Not Used in SUA
0x03	Unsupported Message Class
0x04	Unsupported Message Type
0x05	Unsupported Traffic Handling Mode
0x06	Unexpected Message
0x07	Protocol Error
0x08	Not used in SUA
0x09	Invalid Stream Identifier
0x0a	Not used in SUA
0x0b	Not used in SUA
0x0c	Not used in SUA
0x0d	Refused - Management Blocking
0x0e	ASP Identifier Required
0x0f	Invalid ASP Identifier
0x10	Not Used in SUA
0x11	Invalid Parameter Value
0x12	Parameter Field Error
0x13	Unexpected Parameter
0x14	Destination Status Unknown
0x15	Invalid Network Appearance
0x16	Missing Parameter
0x17	Routing Key Change Refused
0x18	Not Used in SUA
0x19	Invalid Routing Context
0x1a	No Configured AS for ASP
0x1b	Subsystem Status Unknown

The "Invalid Version" error is sent if a message was received with an invalid or unsupported version. The Error message contains the

supported version in the Common header. The Error message could optionally provide the supported version in the Diagnostic information area.

The "Unsupported Message Class" error is sent if a message with an unexpected or unsupported Message Class is received.

The "Unsupported Message Type" error is sent if a message with an unexpected or unsupported Message Type is received.

The "Unsupported Traffic Handling Mode" error is sent by a SGP if an ASP sends an ASP Active message with an unsupported Traffic Mode Type or a Traffic Mode Type that is inconsistent with the presently configured mode for the Application Server. An example would be a case in which the SGP did not support loadsharing.

The "Unexpected Message" error MAY be sent if a defined and recognized message is received that is not expected in the current state (in some cases the ASP may optionally silently discard the message and not send an Error message). For example, silent discard is used by an ASP if it received a DATA message from an SGP while it was in the ASP-INACTIVE state. If the Unexpected message contained Routing Context(s), the Routing Context(s) SHOULD be included in the Error message.

The "Protocol Error" error is sent for any protocol anomaly (i.e., reception of a parameter that is syntactically correct but unexpected in the current situation.

The "Invalid Stream Identifier" error is sent if a message is received on an unexpected SCTP stream.

The "Refused - Management Blocking" error is sent when an ASP Up or ASP Active message is received and the request is refused for management reasons (e.g., management lockout"). If this error is in response to an ASP Active message, the Routing Context(s) in the ASP Active message SHOULD be included in the Error message.

The "ASP Identifier Required" is sent by a SGP in response to an ASP Up message that does not contain an ASP Identifier parameter when the SGP requires one. The ASP SHOULD resend the ASP Up message with an ASP Identifier.

The "Invalid ASP Identifier" is send by a SGP in response to an ASP Up message with an invalid (i.e., non-unique) ASP Identifier.

The "Invalid Parameter Value " error is sent if a message is received with an invalid parameter value (e.g., a DUPU message was received with a Mask value other than "0".

The "Parameter Field Error" would be sent if a message is received with a parameter having a wrong length field.

The "Unexpected Parameter" error would be sent if a message contains an invalid parameter.

The "Destination Status Unknown" Error MAY be sent if a DAUD is received at an SG enquiring of the availability/congestion status of a destination, and the SG does not wish to provide the status (e.g., the sender is not authorized to know the status). For this error, the invalid or unauthorized Point Code(s) MUST be included along with the Network Appearance and/or Routing Context associated with the Point Code(s).

The "Invalid Network Appearance" error is sent by a SGP if an ASP sends a message with an invalid (unconfigured) Network Appearance value. For this error, the invalid (unconfigured) Network Appearance MUST be included in the Network Appearance parameter.

The "Missing Parameter" error would be sent if a mandatory parameter were not included in a message.

The "Invalid Routing Context" error would be sent by a SG if an ASP sends a message with an invalid (unconfigured) Routing Context value. The Error message could optionally provide the invalid Routing Context in the Diagnostic Information area.

The "No Configured AS for ASP" error is sent if a message is received from a peer without a Routing Context parameter and it is not known by configuration data, which Application Servers are

referenced.

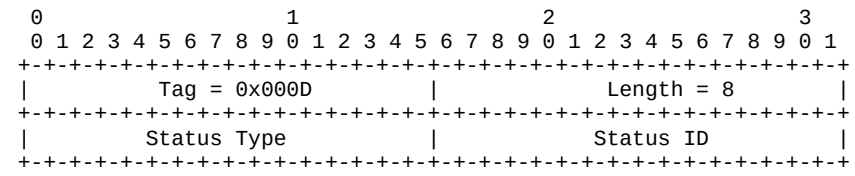
The "Routing Key Change Refused" error is sent when the SG refuses a change in the Routing Key parameters.

The "Destination Status Unknown" Error MAY be sent if a DAUD is received at an SG enquiring of the availability or congestion status of a destination, and the SG does not wish to provide the status (e.g., the sender is not authorized to know the status). For this error, the invalid or unauthorized Point Code(s) MUST be included along with the Network Appearance and Routing Context associated with the Point Code(s).

The "Subsystem Status Unknown" Error MAY be sent if a DAUD is received at an SG enquiring of the availability or congestion status of a subsystem, and the SG does not wish to provide the status (e.g., the sender is not authorized to know the status). For this error, the invalid or unauthorized Point Code and Subsytstem Number MUST be included along with the Network Appearance and Routing Context associated with the Point Code and Subsystem Number.

3.9.13 Status

The Status parameter identifies the type of the status that is being notified and the Status ID.



The valid values for Status Type (16 bit unsigned integer) are:

1 Application Server state change (AS_State_Change)
2 Other

The Status ID parameter contains more detailed information for the notification, based on the value of the Status Type.

If the Status Type is AS_STATE_CHANGE, then the Status ID (16 bit unsigned integer) values are:

1 reserved
2 Application Server Inactive (AS-Inactive)
3 Application Server Active (AS-Active)
4 Application Server Pending (AS-Pending)

These notifications are sent from an SGP to an ASP upon a change in status of a particular Application Server. The value reflects the new state of the Application Server.

If the Status Type is "Other", then the following Status Information values are defined:

1 Insufficient ASP resources active in AS
2 Alternate ASP Active
3 ASP failure

These notifications are not based on the SGP reporting the state change of an ASP or AS. In the Insufficient ASP Resources case, the SGP is indicating to an "Inactive" ASP(s) in the AS that another ASP is required to handle the load of the AS (Load-sharing mode or Broadcast mode). For the Alternate ASP Active case, an ASP is informed when an alternate ASP transitions to the ASP-Active state in Over-ride mode.

3.9.14 Not Used in SUA

Parameter ID 0x000E is not used in SUA.

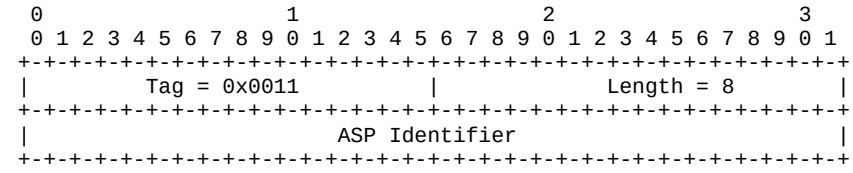
3.9.15 Not Used in SUA

Parameter ID 0x000F is not used in SUA.

3.9.16 Not Used in SUA

Parameter ID 0x0010 is not used in SUA.

3.9.17 ASP Identifier



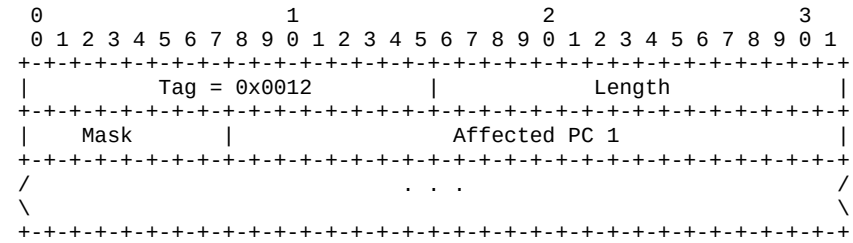
ASP Identifier field: 32-bits (unsigned integer)

The ASP Identifier field contains a unique value that is locally significant amoung the ASPs that support an AS. The SGP should save the ASP Identifier to be used, if necessary, with the Notify message (see Section 3.7.2).

The optional ASP Identifier parameter would contain a unique value that is locally significant among the ASPs that support an AS. The SGP should save the ASP Identifier to be used, if necessary, with the Notify message (see Section 3.3.3.2).

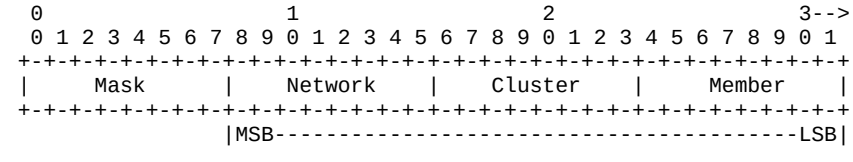
3.9.18 Affected Point Code

The Affected Point Code Destinations parameter contains a list of Affected Point Code fields, each a three-octet parameter to allow for 14-, 16- and 24-bit binary formatted SS7 Point Codes. Affected Point Codes that are less than 24-bits are padded on the left to the 24-bit boundary.

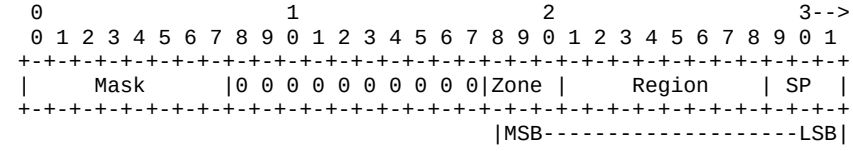


The encoding is shown below for ANSI and ITU Point Code examples.

ANSI 24-bit Point Code:



ITU 14-bit Point Code:



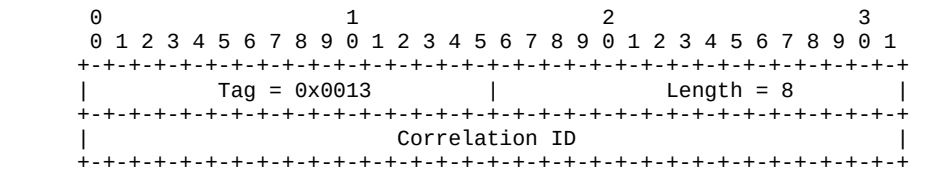
It is OPTIONAL for an implementation to generate an Affected Point Code parameter with more than on Affected PC but the implementation MUST accept and process an Affected Point Code parameter with more than one Affected PC.

Mask: 8-bits

The Mask parameter can be used to identify a contiguous range of Affected Destination Point Codes, independent of the point code format. Identifying a contiguous range of Affected PCs may be useful when reception of an MTP3 management message or a linkset event simultaneously affects the availability status of a series of destinations at an SG.

The Mask parameter is an integer representing a bit mask that can be applied to the related Affected PC field. The bit mask identifies how many bits of the Affected PC field are significant and which are effectively "wild-carded". For example, a mask of "8" indicates that the last eight bits of the PC is "wild-carded". For an ANSI 24-bit Affected PC, this is equivalent to signalling that all PCs in an ANSI Cluster are unavailable. A mask of "3" indicates that the last three bits of the PC is "wild-carded". For a 14-bit ITU Affected PC, this is equivalent to signalling that an ITU Region is unavailable.

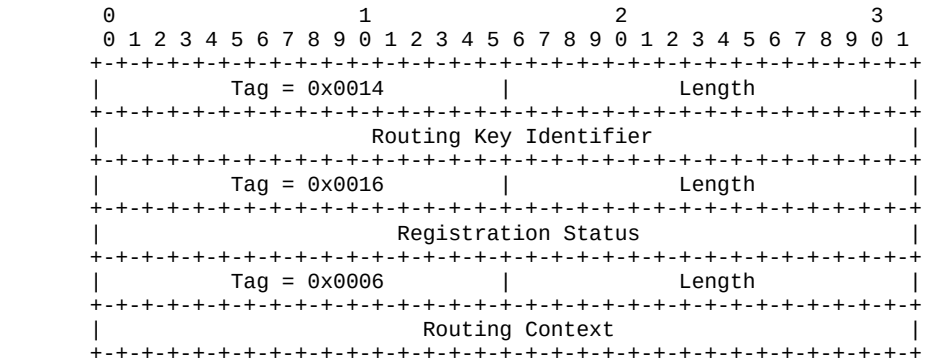
3.9.19 Correlation ID



The Correlation ID is a 32-bit identifier that is attached to CLDT messages to indicate to a newly entering ASP in a Broadcast AS where in the traffic flow of CLDT messages the ASP is joining. It is attached to the first CLDT message sent to an ASP by an SG after sending an ASP Active Ack or otherwise starting traffic to an ASP. The Correlation ID is only significant within a Routing Context.

Implementation note: Correlation ID parameter can be use for features like Synchronisation of ASPs/SGPs in a Broadcast Mode AS/SG; avoid message duplication and mis-sequencing in case of failover of association from one ASP/SGP to other ASP/SGP etc.

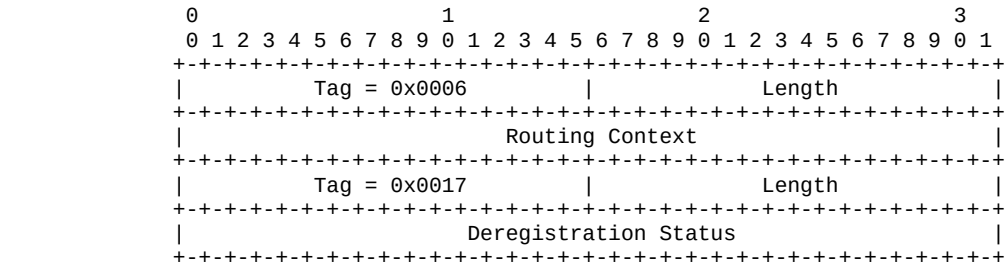
3.9.20 Registration Result



Routing Key Identifier contains the same TLV formatted paramter value as found in the matching Routing Key parameter in the REG REQ message.

Routing Context contains the same TLV formatted Routing Context parameter for the associated Routing Key if the registration was successful. It is set to "0" if the registration was not successful.

3.9.21 Deregistration Result



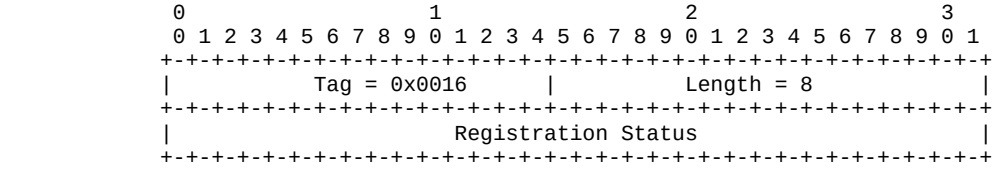
Routing Context: 32-bit integer

Routing Context contains the Routing Context value of the matching Routing key to deregister, as found in the DEREG REQ message.

Deregistration Status: 32-bit integer

Deregistration Status parameter indicates the success or the reason for failure of the deregistration.

3.9.22 Registration Status



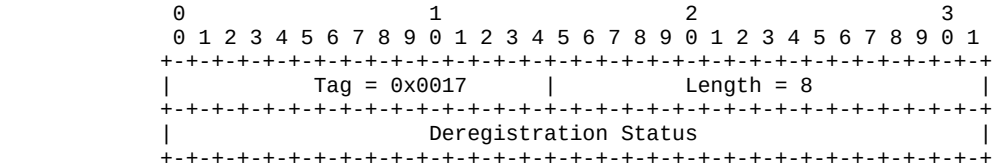
Registration Status: 32-bits (unsigned integer)

The Registration Status field indicates the success or the reason for failure of a registration request.

Its values may be:

0	Successfully Registered
1	Error - Unknown
2	Error - Invalid Destination Address
3	Error - Invalid Network Appearance
4	Error - Invalid Routing Key
5	Error - Permission Denied
6	Error - Cannot Support Unique Routing
7	Error - Routing Key not Currently Provisioned
8	Error - Insufficient Resources
9	Error - Unsupported RK parameter Field
10	Error - Unsupported/Invalid Traffic Mode Type

3.9.23 Deregistration Status



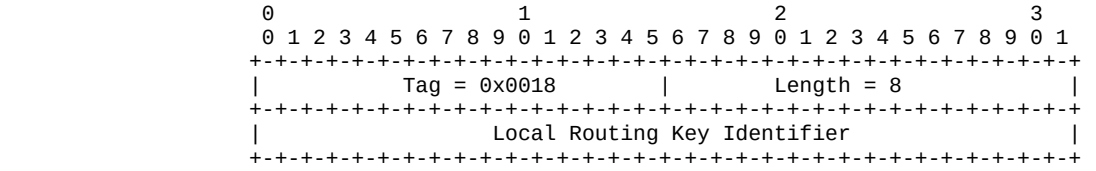
Deregistration Status: 32-bit integer

The Deregistration Result Status field indicates the success or the reason for failure of the deregistration.

Its values may be:

0	Successfully Deregistered
1	Error - Unknown
2	Error - Invalid Routing Context
3	Error - Permission Denied
4	Error - Not Registered
5	Error - ASP Currently Active for Routing Context

3.9.24 Local Routing Key Identifier



The Local Routing Key Identifier field is a 32-bits unsigned integer. The Identifier value is assigned by the ASP and is used to correlate the response in a REG RSP message with the original registration request. The Identifier value must remain unique until the REG RSP message is received.

3.10 SUA-Specific parameters

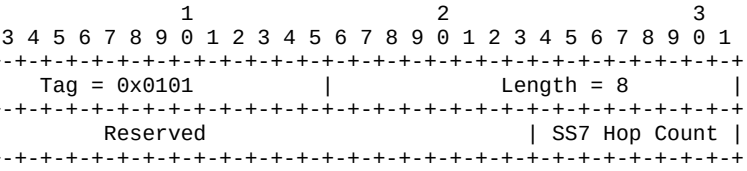
These TLV parameters are specific to the SUA protocol.

Parameter Name	Parameter ID
SS7 Hop Counter	0x0101
Source Address	0x0102
Destination Address	0x0103
Source Reference Number	0x0104
Destination Reference Number	0x0105
SCCP Cause	0x0106
Sequence Number	0x0107
Receive Sequence Number	0x0108
ASP Capabilities	0x0109
Credit	0x010A
Data	0x010B
User/Cause	0x010C
Network Appearance	0x010D
Routing Key	0x010E
DRN Label	0x010F
TID Label	0x0110
Address Range	0x0111
SMI	0x0112
Importance	0x0113

Message Priority	0x0114
Protocol Class	0x0115
Sequence Control	0x0116
Segmentation	0x0117
Congestion Level	0x0118

Destination/Source Address Sub-Parameters	
Global Title	0x8001
Point Code	0x8002
Subsystem Number	0x8003
IPv4 Address	0x8004
Hostname	0x8005
IPv6 Addresses	0x8006

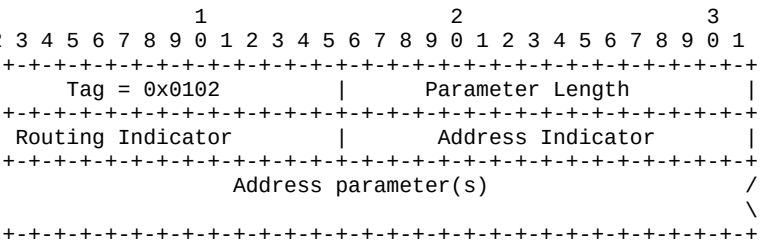
3.10.1 SS7 Hop counter



SS7 Hop Counter (3.18/Q.713)

The value of the SS7 Hop Counter is decremented with each global title translation and is in the range 15 to 1.

3.10.2 Source Address



The following combinations of address parameters are valid:

- Global Title (e.g. E.164 number) + optional PC and/or SSN, SSN may be zero, when routing is done on Global Title
- SSN (non-zero) + optional PC and/or Global Title, when routing is done on PC + SSN. The PC is mandatory in the source address when sending from SGP to ASP, and in the destination address when sending from ASP to SGP to reach the SS7 SEP.

- Hostname + optional SSN, when routing is done by Hostname
- SSN (non-zero) and optional IP address (IPv4 or IPv6) when routing is done on IP address + SSN

3.10.2.1 Routing Indicator

The following values are valid for the routing indicator:

Reserved	0
Route on Global Title	1
Route on SSN + PC	2
Route on Hostname	3
Route on SSN + IP Address	4

The routing indicator determines which address parameters need to be present in the address parameters field.

3.10.2.2 Address Indicator

This parameter is needed for interworking with SS7 networks. The address indicator specifies what address parameters are actually received in the SCCP address from the SS7 network, or are to be populated in the SCCP address when the message is sent into the SS7 network. The value of the routing indicator needs to be taken into account. It is used in the ASP to SG direction. For example, the PC parameter is present in the destination address of the CLDT sent from ASP->SG, but bit 2 is set to "0" meaning "do not populate this in the SCCP called party address". The effect is that the SG only uses the PC to populate the MTP routing label DPC field, but does not include it in the SCCP called party address.

In the SG->ASP direction, the source address PC parameter is present (PC of SS7 SEP). However, this may have been populated from the OPC in the received MTP routing label, not from the PC field in the SCCP calling party address. In this case, bit 2 = "0" denotes that. The AI gives further instructions to the SG how and when to populate the SCCP addresses; in the SG->ASP direction, the AI gives information to the ASP as to what was actually present in the received SCCP addresses.

The address indicator is coded as follows:

Bit 1 is used to indicate inclusion of the SSN

0 Do not include SSN when optional
1 Include SSN

Bit 2 is used to indicate inclusion of the PC

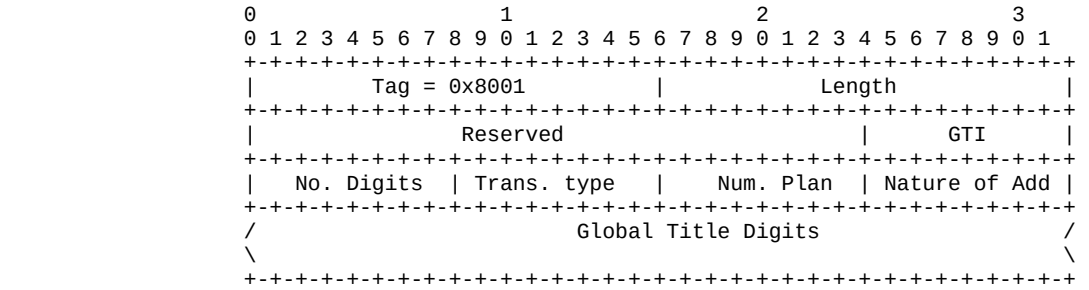
0 Do not include PC, regardless of the routing indicator value
1 Include PC

Bit 3 is used to indicate inclusion of the Global Title

0 Do not include GT when optional (routing indicator /= 1)
1 Include GT

The remaining bits are spare and SHOULD be coded zero, and MUST be ignored by the receiver.

3.10.2.3 Global Title



Number of Digits:

This is the number of digits contained in the Global Title.

GTI (defined in chapter 3.4.2.3 of Q.713):

0000	Reserverd
0001	Nature of Address is ignored. Translation Type = Unknown and Numbering Plan = E.164 (value 1).
0010	This is most commonly used in North American networks. The Translation Type implicitly determines Nature of Address and Numbering Plan. This data can be configured in the SG. The number of digits is always even and determined by the SCCP address length.
0011	Numbering Plan and Translation Type are tak is implicitly assumed that the Nature of Address = Unknown.
0100	This format is used in international networ commonly in networks outside North America. All information to populate the source address is present in the SCCP Address.

Translation type:

0	Unknown
1 - 63	International services
64 - 127	Spare
128 > 254	National network specific
255	Reserved

Numbering Plan:

0	unknown
1	ISDN/telephony numbering plan (Recommendations E.163 and E.164)
2	generic numbering plan

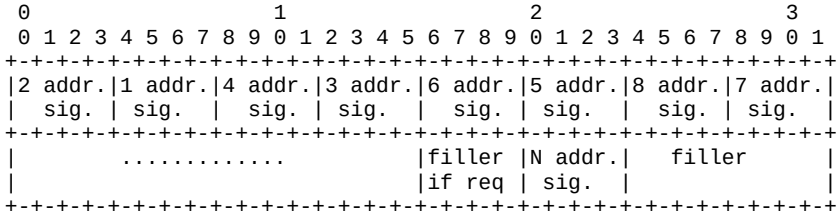
3	data numbering plan (Recommendation X.121)
4	telex numbering plan (Recommendation F.69)
5	maritime mobile numbering plan (Recommendations E.210, E.211)
6	land mobile numbering plan (Recommendation E.212)
7	ISDN/mobile numbering plan (Recommendation E.214)
8 - 13	spare
14	private network or network-specific numbering plan
15 - 126	spare
127	reserved.

Nature of Address:

```
  0         unknown
  1         subscriber number
  2         reserved for national use
  3         national significant number
  4         international number
  5 - 255   Spare
```

Global Title:

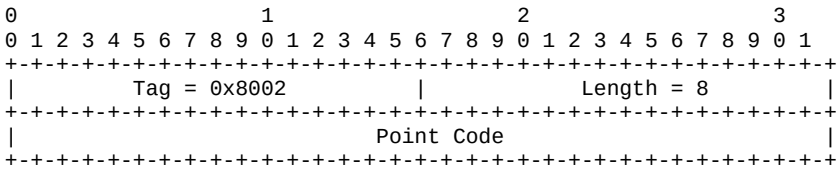
Octets contain a number of address signals and possibly filler as shown:



All filler bits SHOULD be set to 0.

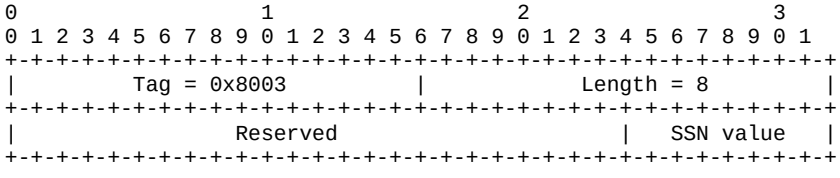
Address signals to be coded as defined in ITU-T Q.713 Section 3.4.2.3.1.

3.10.2.4 Point Code



See chapter 3.9.18 Affected Point Code for the layout of the Point Code field.

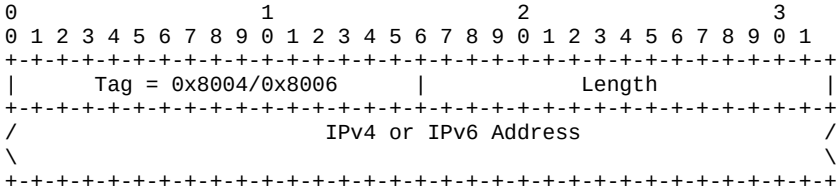
3.10.2.5 Subsystem Number



The internationally standardized SSN values are described in chapter 3.4.2.2 of Q.713.

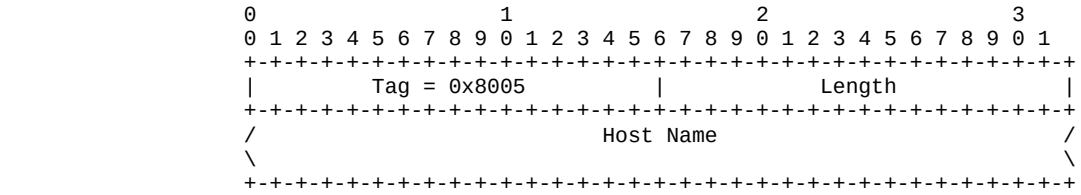
3.10.2.6 IP Addresses

The IP address formats can use different tags. It should be noted that if the source address is in a certain IP version, the destination address should also be in the same IP version.



Note: The tag value 0x8004 is for an IPv4 address and 0x8006 is for IPv6.

3.10.2.7 Hostname

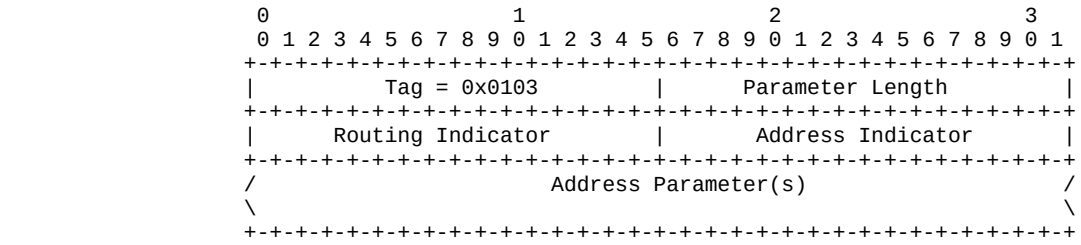


Host Name: variable length

This field contains a host name in "host name syntax" per RFC 1123 Section 2.1 [1123]. The method for resolving the host name is out of scope for this document.

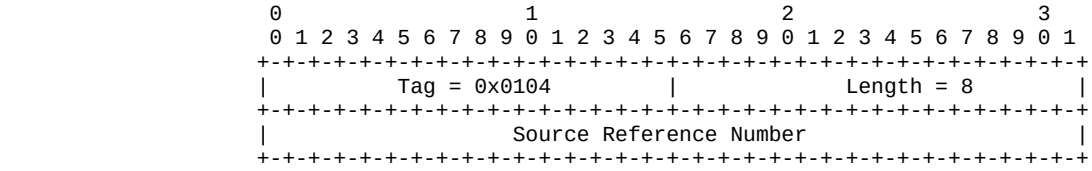
Note: At least one null terminator is included in the Host Name string and must be included in the length.

3.10.3 Destination Address



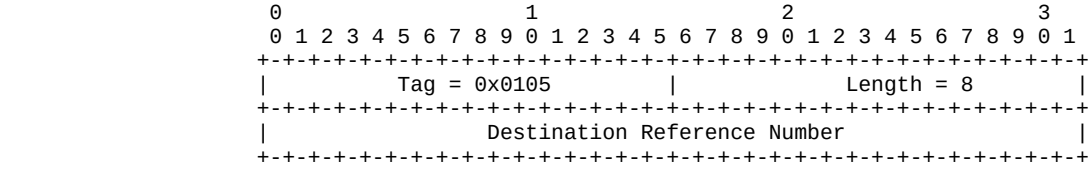
The format of this parameter is identical to the Source Address parameter.

3.10.4 Source Reference Number



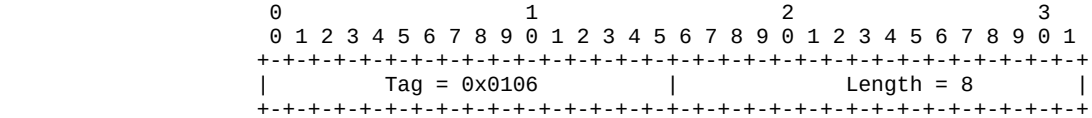
The source reference number is a 4 octet long integer. This is allocated by the source SUA instance.

3.10.5 Destination Reference Number



The destination reference number is a 4 octet long integer. This is allocated by the destination SUA instance.

3.10.6 SCCP Cause



```
      |         Reserved              |   Cause Type  |  Cause Value  |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```


This parameter bundles the SCCP parameters Release cause, Return cause, Reset cause, Error cause and Refusal cause.

Cause Type can have the following values:

Return Cause	0x1
Refusal Cause	0x2
Release Cause	0x3
Reset Cause	0x4
Error Cause	0x5

Cause Value contains the specific cause value. Below gives examples for ITU SCCP values. ANSI references can be found in ANSI T1.112.3

Cause value in SUA message	Correspondence with Reference SCCP parameter	
CLDR	Return Cause	ITU-T Q.713 Chap 3.12
COREF	Refusal Cause	ITU-T Q.713 Chap 3.15
RELRE	Release Cause	ITU-T Q.713 Chap 3.11
RESRE	Reset Cause	ITU-T Q.713 Chap 3.13
ERR	Error Cause	ITU-T Q.713 Chap 3.14

3.10.7 Sequence Number

```
       0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |          Tag = 0x0107         |             Length = 8        |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |         Reserved              |  Rec Seq Num|M| Sent Seq Num  |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

This parameter is used to indicate whether "more" data will follow in subsequent CODT messages, and/or to number each CODT message sequentially for the purpose of flow control. It contains the received as well as the sent sequence number, P(R) and P(S) in Q.713, chapters 3.7 and 3.9.

As such it can also be used to acknowledge the receipt of data transfers from the peer in case of protocol class 3.

Sent Sequence Number is one octet and is coded as follows:

Bits 2-8 are used to indicate the Send Sequence Number P(S).
Bit 1 (LSB) of octet 1 is spare.

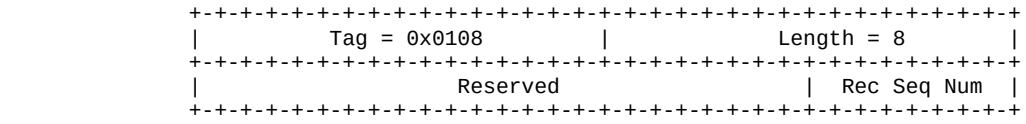
Received Sequence Number is one octet, and is coded as follows:

Bits 2-8 are used to indicate the Received Sequence Number P(R).
Bit 1 (LSB) is used for the more data indication, as follows:

0	no more data
1	more data

3.10.8 Receive Sequence Number

```
       0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```



This parameter is used exclusively for protocol class 3 in the data acknowledgment message to indicate the lower edge of the receiving window. See Q.713, chapter 3.9.

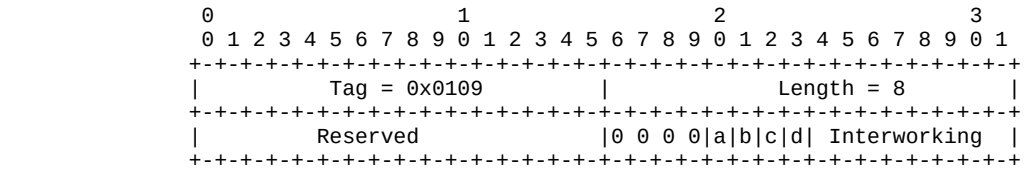
It is a 1 octet long integer coded as follows:

Bits 8-2 are used to indicate the Receive Sequence Number P(R).

Bit 1 is spare.

3.10.9 ASP Capabilities

This parameter is used so that the ASP can report its capabilities regarding SUA for supporting different protocol classes and interworking scenarios.



Flags

a - Protocol Class 3
b - Protocol Class 2
c - Protocol Class 1
d - Protocol Class 0

It is mandatory to support at least Protocol Class 0.

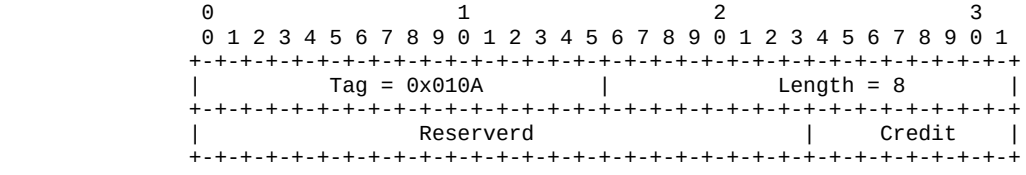
Interworking

Values

0x0 indicates no interworking with SS7 Networks.

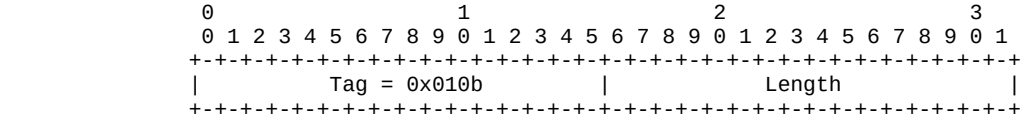
0x1 indicates IP Signalling Endpoint (ASP), interworking with SS7 networks.
0x2 indicates Signalling Gateway.
0x3 indicates relay node support.

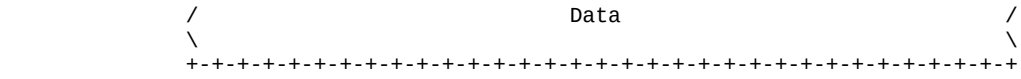
3.10.10 Credit



The length of the credit field is is one octet. See ITU-T Q.713 Chapter 3.10. The parameter is used for protocol class 3 exclusively.

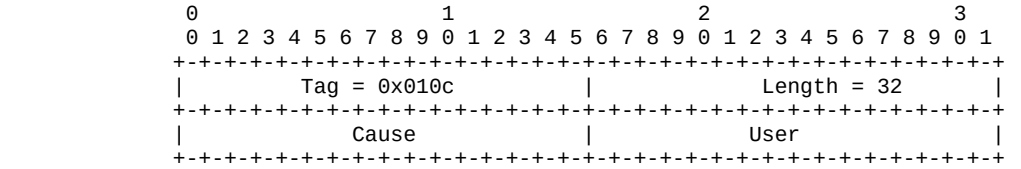
3.10.11 Data





The Data parameter field contains the SS7 SCCP-User application message, for example an INAP/TCAP message.

3.10.12 Cause / User

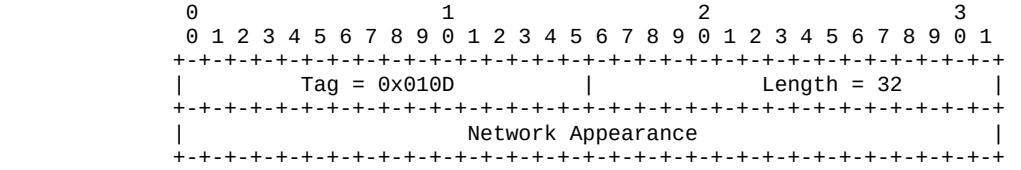


"User" is coded to that SCCP's SI value. There may be several SCCP's at a given point code, each with different SI values, although normally there is only one with SI = 3.

Cause may take the following values

0 remote SCCP unavailable, reason unknown;
1 remote SCCP unequipped;
2 remote SCCP inaccessible;

3.10.13 Network Appearance

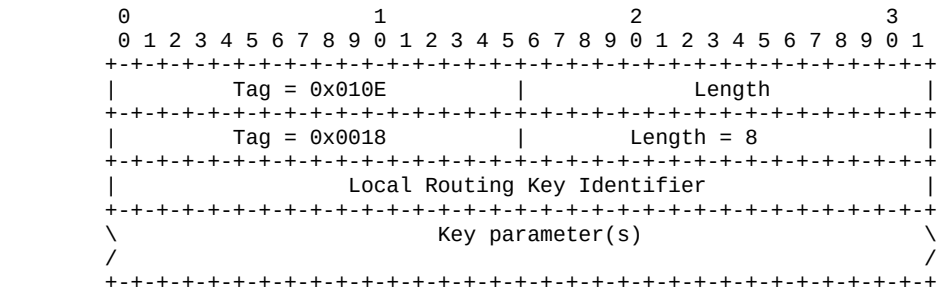


Network Appearance field: 32-bits (unsigned integer)

The Network Appearance field identifies the SS7 network context for the Routing Key. The Network Appearance value is of local significance only, coordinated between the SG and ASP. Therefore, in the case where the ASP is connected to more than one SG, the same SS7 Network context may be identified by different Network Appearance values depending upon to which SG the ASP is registering.

In the Routing Key, the Network Appearance identifies the SS7 Point Code and Global Title Translation Type format used, and the SCCP and possibly the SCCP-User protocol (type, variant and version) used within the specific SS7 network.

3.10.14 Routing Key



Local Routing Key Identifier field: 32-bits (unsigned integer)

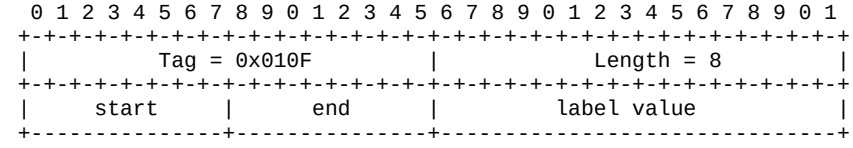
Key field: variable

The Key field contains the following parameters:

Parameter	
Traffic Mode Type	Optional
Network Appearance	Optional *1
Source Address	Optional
Destination Address	Optional
Address Range	Optional

Note 1: The Network Appearance parameter must be included in the Routing Key when the ASP is able to register in multiple SS7 Network contexts.

3.10.15 DRN Label

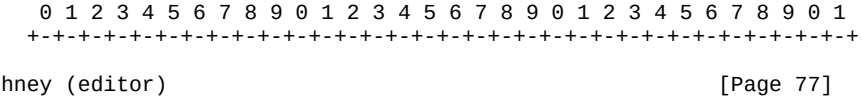


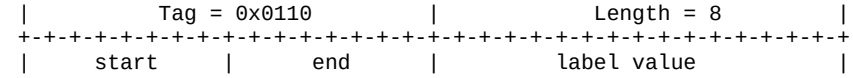
The Start parameter is the start position of label, between 0 (LSB) and 23 (MSB).

The End parameter is the end position of label, between 0 (LSB) and 23 (MSB).

Label value is a 16-bit interger, which is unique across an AS.

3.10.16 TID Label





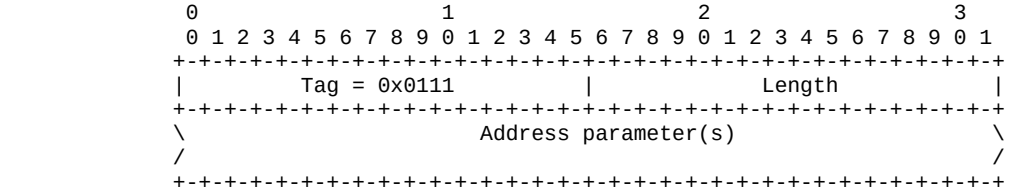
```
   +---------------+---------------+-------------------------------+
```

The Start parameter is the start position of label, between 0 (LSB) and 31 (MSB).

The End parameter is the end position of label, between 0 (LSB) and 31 (MSB).

Label value is a 16-bit interger, which is unique across an AS.

3.10.17 Address Range



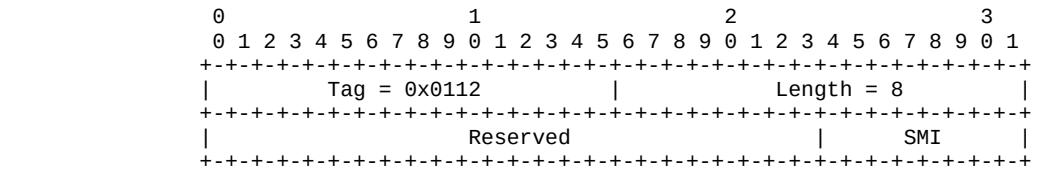
Address field:

The Address field the following parameters:

Parameter	
Source Address	Optional *1
Destination Address	Optional *1

Note 1: The Address field must contain pairs of Source Addresses or pairs of Destination Addresses but MUST NOT mix Source Addresses with Destination Addresses in the same Address field.

3.10.18 SMI

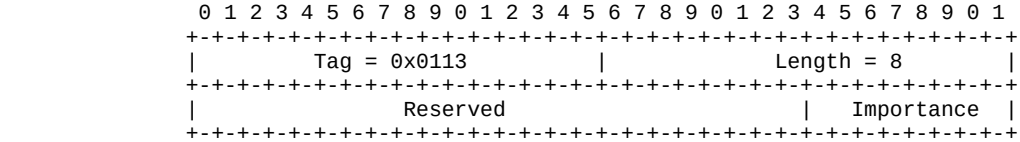


Subsystem Multiplicity Indicator (SMI) can have the following values:

0x00	Reserved/Unknown
0x01	Solitary
0x02	Duplicated

0x03	Triplicated
0x04	Quadruplicated
...	...
0xff	Unspecified

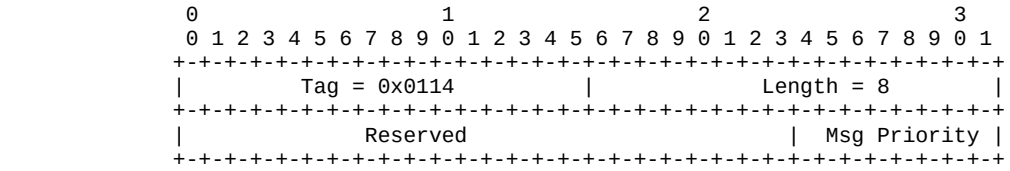
3.10.19 Importance



Importance (3.19/Q.713)

Possible values of the Importance Parameter are between 0 and 7, where the value of 0 indicates the least important and 7 indicates the most important.

3.10.20 Message Priority (or Priority)

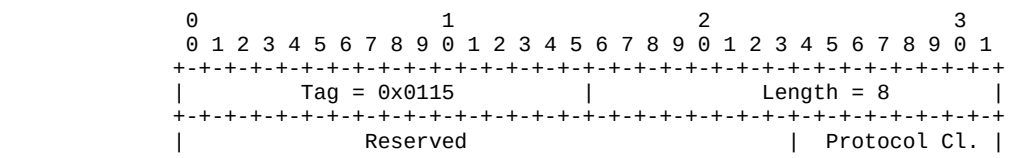


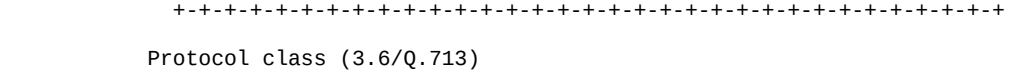
Priority

Priority value ranges from 0 to 3. If the Priority value has not been specified by the SCCP user, it should be set to 0xFF. The SG MAY take the priority into account for determining the MTP message priority. In the all-IP case, this parameter MAY be used.

The Message Priority parameter is optional in the CLDT, CLDR, CORE, COAK and CODT messages. However, for networks, which support Message Priority message priorities (e.g, ANSI), this parameter MUST be included but it is not required for those which don't (e.g., International).

3.10.21 Protocol Class





Protocol class (3.6/Q.713)

Bits 1-2 indicate the protocol class.

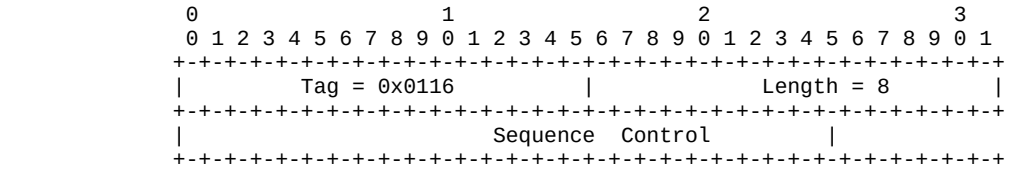
Value	Description
0	Class 0 (connectionless service)
1	Class 1 (connectionless service)
2	Class 2 (connection-oriented service)
3	Class 3 (connection-oriented service)

Bit 8 indicates the use of the return on error procedure.

Value	Description
0x0	No special options
0x1	Return message on error

Bits 3-7 are spare and SHOULD be coded zero, and MUS ignored by the receiver.

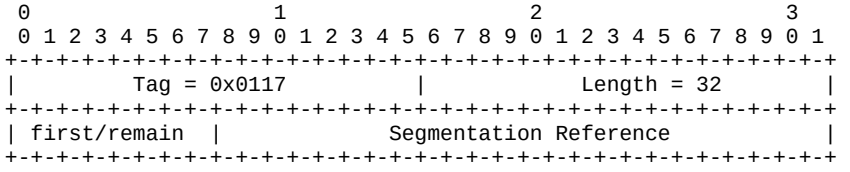
3.10.22 Sequence Control



Sequence Control (1.1.2/Q.714)

The field is coded with the value of the sequence control parameter associated with a group of messages and are chosen so as to ensure proper loadsharing of message groups over SLS values while ensuring that sequence control values within message groups have the sequence control value coded with the same value as the initial message of the message group.

3.10.23 Segmentation



The first/remaining segments field is formatted as follows:

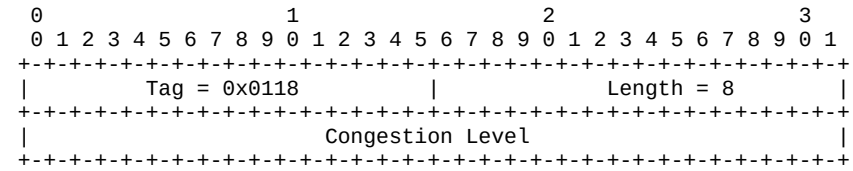
bit 8 (MSB) : indicates whether this is the first segment (1) or not (0)

bits 1-7: indicate the number of remaining segments, value between 0 and 15

The field would thus be coded 1000 0000 (first, no remaining segments) for a non-segmented CLDT.

The segmentation reference field is a 3 byte integer, assigned by the ASP.

3.10.24 Congestion Level



Congestion Level field: 8-bits (unsigned integer)

The Congestion Level field contains the level at which congestion has occured.

When the Congestion Level parameter is included in a SCON message that corresponds to an N-PCSTATE primitive, the Congestion Level field indicates the MTP congestion level experienced by the local or affected signalling point as indicated by the Affected Point Code(s) also in the SCON message. In this case, valid values for the Congestion Level field are as follows:

0 No Congestion or Undefined
1 Congestion Level 1
2 Congestion Level 2
3 Congestion Level 3

When the Congestion Level parameter is included in a SCON messagethat corresponds to an N-STATE primitive, the Congestion Level field indicates the SCCP restricted importance level experienced by the local or affected subsystem as indicated by the Affected Point Code and Subsystem Number also in the SCON message. In this case, valid values for the Congestion Level field range from 0 to 7, where 0 indicates the least congested and 7 indicates the most congested subsystem.

4. Procedures

The SUA layer needs to respond to various local primitives it receives from other layers as well as the messages that it receives

from the peer SUA layer. This section describes the SUA procedures in response to these events.

4.1 Procedures to Support the SUA-User Layer

4.1.1 Receipt of Primitives from SCCP

When an SCCP Subsystem Management (SCMG) message is received from the SS7 network, the SGP needs to determine whether there are concerned Application Servers interested in subsystem status changes. The SUA management function is informed with the N-State or N-Coord primitive upon which it formats and transfers the applicable SNMM message to the list of concerned ASPs using stream ID "0".

When MTP-3 Management indications are received (MTP-PAUSE, MTP-RESUME, MTP-STATUS), SCCP Subsystem Management determines whether there are concerned local SCCP-users. When these local SCCP-users are in fact Application Servers, serviced by ASPs, SUA management is informed with the N-PCSTATE indication primitive upon which it formats and transfers the applicable SNM message (DUNA, DAVA, DRST or SCON) to the list of concerned ASPs using stream ID "0".

The SUA message distribution function determines the Application Server (AS) based on comparing the information in the N-UNITDATA request primitive with a provisioned Routing Key.

From the list of ASPs within the AS table, an ASP in the ASP-ACTIVE state is selected and a DATA message is constructed and issued on the corresponding SCTP association. If more than one ASP is in the ASP-ACTIVE state (i.e., traffic is to be load-shared across more than one ASP), one of the ASPs in the ASP_ACTIVE state is selected from the list. If the ASPs are in Broadcast Mode, all active ASPs will be selected and the message sent to each of the active ASPs. The selection algorithm is implementation dependent but could, for example, be round robin or based on the SLS. The appropriate selection algorithm must be chosen carefully as it is dependent on application assumptions and understanding of the degree of state coordination between the ASP_ACTIVE ASPs in the AS.

In addition, the message needs to be sent on the appropriate SCTP stream, again taking care to meet the message sequencing needs of the signalling application. DATA messages MUST be sent on an SCTP stream other than stream '0' when there is more than one stream.

When there is no Routing Key match, or only a partial match, for an incoming SS7 message, a default treatment MAY be specified. Possible solutions are to provide a default Application Server at the SGP that directs all unallocated traffic to a (set of) default ASP(s), or to drop the message and provide a notification to Layer Management in an M-ERROR indication primitive. The treatment of unallocated traffic is implementation dependent.

4.2 Receipt of Primitives from the Layer Management

On receiving primitives from the local Layer Management, the SUA layer will take the requested action and provide an appropriate response primitive to Layer Management.

An M-SCTP_ESTABLISH request primitive from Layer Management at an ASP or IPSP will initiate the establishment of an SCTP association. The SUA layer will attempt to establish an SCTP association with the remote SUA peer by sending an SCTP-ASSOCIATE primitive to the local SCTP layer.

When an SCTP association has been successfully established, the SCTP will send an SCTP-COMMUNICATION_UP notification primitive to the local SUA layer. At the SGP or IPSP that initiated the request, the SUA layer will send an M-SCTP_ESTABLISH confirm primitive to Layer

Management when the association setup is complete. At the peer SUA layer, an M-SCTP_ESTABLISH indication primitive is sent to Layer Management upon successful completion of an incoming SCTP association setup.

An M-SCTP_RELEASE request primitive from Layer Management initates the shutdown of an SCTP association. The SUA layer accomplishes a graceful shutdown of the SCTP association by sending an SCTP-SHUTDOWN primitive to the SCTP layer.

When the graceful shutdown of the SCTP association has been accomplished, the SCTP layer returns an SCTP-SHUTDOWN_COMPLETE notification primitive to the local SUA layer. At the SUA Layer that initiated the request, the SUA layer will send an M-SCTP_RELEASE confirm primitive to Layer Management when the association shutdown is complete. At the peer SUA Layer, an M-SCTP_RELEASE indication primitive is sent to Layer Management upon abort or successful shutdown of an SCTP association.

An M-SCTP_STATUS request primitive supports a Layer Management query of the local status of a particular SCTP association. The SUA layer simply maps the M-SCTP_STATUS request primitive to an SCTP-STATUS primitive to the SCTP layer. When the SCTP responds, the SUA layer maps the association status information to an M-SCTP_STATUS confirm primitive. No peer protocol is invoked.

Similar LM-to-SUA-to-SCTP and/or SCTP-to-SUA-to-LM primitive mappings can be described for the various other SCTP Upper Layer primitives in RFC 2960 [2960] such as INITIALIZE, SET PRIMARY, CHANGE HEARTBEAT, REQUEST HEARTBEAT, GET SRTT REPORT, SET FAILURE THRESHOLD, SET PROTOCOL PARAMETERS, DESTROY SCTP INSTANCE, SEND FAILURE, AND NETWORK STATUS CHANGE. Alternatively, these SCTP Upper Layer primitives (and Status as well) can be considered for modeling purposes as a Layer Management interaction directly with the SCTP Layer.

M-NOTIFY indication and M-ERROR indication primitives indicate to Layer Management the notification or error information contained in a received SUA Notify or Error message respectively. These indications can also be generated based on local SUA events.

An M-ASP_STATUS request primitive supports a Layer Management query of the status of a particular local or remote ASP. The SUA layer responds with the status in an M-ASP_STATUS confirm primitive. No SUA peer protocol is invoked. An M-AS_STATUS request supports a Layer Management query of the status of a particular AS. The SUA responds with an M-AS_STATUS confirm primitive. No SUA peer protocol is invoked.

M-ASP_UP request, M-ASP_DOWN request, M-ASP_ACTIVE request and M-ASP_INACTIVE request primitives allow Layer Management at an ASP to initiate state changes. Upon successful completion, a corresponding confirm primitive is provided by the SUA layer to Layer Management. If an invocation is unsuccessful, an Error indication primitive is provided in the primitive. These requests result in outgoing ASP Up, ASP Down, ASP Active and ASP Inactive messages to the remote SUA peer at an SGP or IPSP.

4.2.1 Receipt of SUA Peer Management Messages

Upon successful state changes resulting from reception of ASP Up, ASP Down, ASP Active and ASP Inactive messages from a peer SUA, the SUA layer MAY invoke corresponding M-ASP_UP, M-ASP_DOWN, M-ASP_ACTIVE and M-ASP_INACTIVE, M-AS_ACTIVE, M-AS_INACTIVE, and M-AS_DOWN indication primitives to the local Layer Management.

M-NOTIFY indication and M-ERROR indication primitives indicate to Layer Management the notification or error information contained in a received SUA Notify or Error message. These indications can also be generated based on local SUA events.

All non-Transfer messages, except BEAT and BEAT Ack, SHOULD be sent with sequenced delivery to ensure ordering. All non-Transfer messages, with the exception of ASPTM, BEAT and BEAT Ack messages SHOULD be sent on SCTP stream '0'. ASPTM messages MAY be sent on one of the streams used to carry data traffic related to the Routing Context(s), to minimize possible message loss. BEAT and BEAT Ack messages MAY be sent using out-of-order delivery, and MAY be sent on any stream.

4.3 AS and ASP State Maintenance

The SUA layer on the SGP maintains the state of each remote ASP, in each Application Server that the ASP is configured to receive traffic, as input to the SUA message distribution function. Similarly, where IPSPs use SUA in a point-to-point fashion, the SUA layer in an IPSP maintains the state of remote IPSPs. For the purposes of the following procedures, only the SGP/ASP case is

described but the SGP side of the procedures also apply to an IPSP sending traffic to an AS consisting of a set of remote IPSPs.

4.3.1 ASP States

The state of each remote ASP, in each AS that it is configured to operate, is maintained in the SUA layer in the SGP. The state of a particular ASP in a particular AS changes due to events. The events include:

* Reception of messages from the peer SUA layer at the ASP;
* Reception of some messages from the peer SUA layer at other ASPs in the AS (e.g., ASP Active message indicating "Override");
* Reception of indications from the SCTP layer; or
* Local Management intervention.

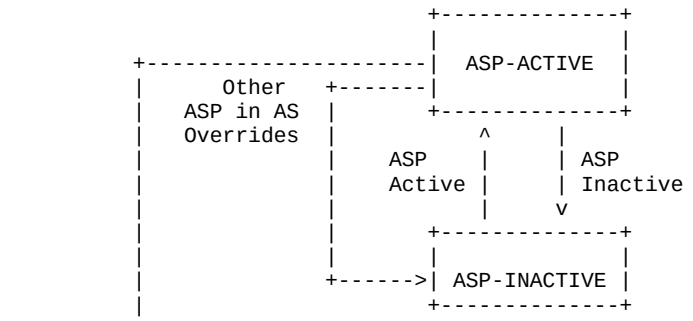
The ASP state transition diagram is shown in Figure 4. The possible states of an ASP are:

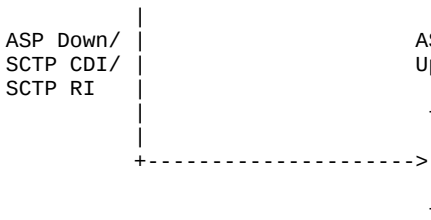
ASP-DOWN: The remote SUA peer at the ASP is unavailable and/or the related SCTP association is down. Initially all ASPs will be in this state. An ASP in this state SHOULD NOT be sent any SUA messages, with the exception of Heartbeat, ASP Down Ack and Error messages.

ASP-INACTIVE: The remote SUA peer at the ASP is available (and the related SCTP association is up) but application traffic is stopped. In this state the ASP SHOULD NOT be sent any CL, CO or SNMM messages for the AS for which the ASP is inactive.

ASP-ACTIVE: The remote SUA peer at the ASP is available and application traffic is active (for a particular Routing Context or set of Routing Contexts).

Figure 4: ASP State Transition Diagram (Per AS)





SCTP CDI: The SCTP CDI denotes the local SCTP layer's Communication Down Indication to the Upper Layer Protocol (SUA) on an SGP. The local SCTP layer will send this indication when it detects the loss of connectivity to the ASP's peer SCTP layer. SCTP CDI is understood as either a SHUTDOWN_COMPLETE notification or COMMUNICATION_LOST notification from the SCTP layer.

SCTP RI: The local SCTP layer's Restart indication to the upper layer protocol (SUA) on an SG. The local SCTP will send this indication when it detects a restart from the ASP's peer SCTP layer.

4.3.2 AS States

The state of the AS is maintained in the SUA layer on the SGP. The state of an AS changes due to events. These events include:

* ASP state transitions
* Recovery timer triggers

The possible states of an AS are:

AS-DOWN: The Application Server is unavailable. This state implies that all related ASPs are in the ASP-DOWN state for this AS. Initially the AS will be in this state. An Application Server is in the AS-DOWN state before it can be removed from a configuration.

AS-INACTIVE: The Application Server is available but no application traffic is active (i.e., one or more related ASPs are in the ASP-INACTIVE state, but none in the ASP-ACTIVE state). The recovery timer T(r) is not running or has expired.

AS-ACTIVE: The Application Server is available and application traffic is active. This state implies that at least one ASP is in the ASP-ACTIVE state.

AS-PENDING: An active ASP has transitioned to ASP-INACTIVE or ASP-DOWN and it was the last remaining active ASP in the AS. A recovery timer T(r) SHOULD be started and all incoming signalling messages SHOULD be queued by the SGP. If an ASP becomes ASP-ACTIVE before T(r) expires, the AS is

moved to the AS-ACTIVE state and all the queued messages will be sent to the ASP.

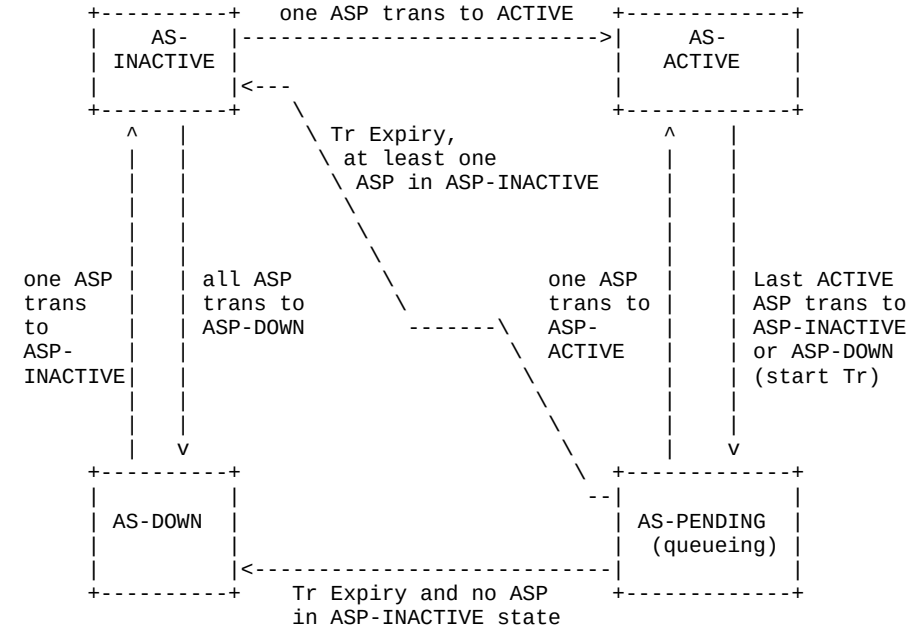
If T(r) expires before an ASP becomes ASP-ACTIVE, and the SGP has no other alternative, the SGP may stop queueing messages and discard all previously queued messages. The AS will move to the AS-INACTIVE state if at least one ASP is in ASP-INACTIVE state, otherwise it will move to AS-DOWN state.

Figure 5 shows an example AS state machine for the case where the AS/ASP data is pre-configured. For other cases where the AS/ASP

configuration data is created dynamically, there would be differences in the state machine, especially at creation of the AS.

For example, where the AS/ASP configuration data is not created until Registration of the first ASP, the AS-INACTIVE state is entered directly upon the first successful REG REQ from an ASP. Another example is where the AS/ASP configuration data is not created until the first ASP successfully enters the ASP-ACTIVE state. In this case the AS-ACTIVE state is entered directly.

Figure 5: AS State Transition Diagram



Tr = Recovery Timer

4.3.2.1 IPSP Considerations

The AS state diagram for the AS-SG case is applicable for IPSP communication.

4.3.3 SUA Management Procedures for Primitives

Before the establishment of an SCTP association the ASP state at both the SGP and ASP is assumed to be in the state ASP-DOWN.

Once the SCTP association is established (see Section 4.2.1) and assuming that the local SUA-User is ready, the local SUA ASP Maintenance (ASPM) function will initiate the relevant procedures, using the ASP Up/ASP Down/ASP Active/ASP Inactive messages to convey the ASP state to the SGP (see Section 4.3.4).

If the SUA layer subsequently receives an SCTP-COMMUNICATION_DOWN or SCTP-RESTART indication primitive from the underlying SCTP layer, it will inform the Layer Management by invoking the M-SCTP_STATUS

indication primitive. The state of the ASP will be moved to ASP-DOWN.

In the case of SCTP-COMMUNICATION_DOWN, the SCTP client MAY try to re-establish the SCTP association. This MAY be done by the SUA layer automatically, or Layer Management MAY re-establish using the M-SCTP_ESTABLISH request primitive.

In the case of an SCTP-RESTART indication at an ASP, the ASP is now considered by its SUA peer to be in the ASP-DOWN state. The ASP, if it is to recover, must begin any recovery with the ASP-Up procedure.

4.3.4 ASPM Procedures for Peer-to-Peer Messages

4.3.4.1 ASP Up Procedures

After an ASP has successfully established an SCTP association to an SGP, the SGP waits for the ASP to send an ASP Up message, indicating that the ASP SUA peer is available. The ASP is always the initiator of the ASP Up message. This action MAY be initiated at the ASP by an M-ASP_UP request primitive from Layer Management or MAY be initiated automatically by an SUA management function.

When an ASP Up message is received at an SGP and internally the remote ASP is in the ASP-DOWN state and not considered locked-out for local management reasons, the SGP marks the remote ASP in the state ASP-INACTIVE and informs Layer Management with an M-ASP_Up indication primitive. If the SGP is aware, via current configuration data, which Application Servers the ASP is configured to operate in, the SGP updates the ASP state to ASP-INACTIVE in each AS that it is a member.

Alternatively, the SGP may move the ASP into a pool of Inactive ASPs available for future configuration within Application Server(s), determined in a subsequent Registration Request or ASP Active procedure. If the ASP Up message contains an ASP Identifier, the SGP should save the ASP Identifier for that ASP. The SGP MUST send an ASP Up Ack message in response to a received ASP Up message even if the ASP is already marked as ASP-INACTIVE at the SGP.

If for any local reason (e.g., management lock-out) the SGP cannot respond with an ASP Up Ack message, the SGP responds to an ASP Up message with an Error message with Reason "Refused - Management Blocking".

At the ASP, the ASP Up Ack message received is not acknowledged. Layer Management is informed with an M-ASP_UP confirm primitive.

When the ASP sends an ASP Up message it starts timer T(ack). If the ASP does not receive a response to an ASP Up message within T(ack), the ASP MAY restart T(ack) and resend ASP Up messages until it

receives an ASP Up Ack message. T(ack) is provisionable, with a default of 2 seconds. Alternatively, retransmission of ASP Up messages MAY be put under control of Layer Management. In this method, expiry of T(ack) results in an M-ASP_UP confirm primitive carrying a negative indication.

The ASP must wait for the ASP Up Ack message before sending any other SUA messages (e.g., ASP Active or REG REQ). If the SGP receives any other SUA messages before ASPUP message is received (other than ASPDN - see section 4.3.4.2), the SGP SHOULD discard them.

If an ASP Up message is received and internally the remote ASP is in the ASP-ACTIVE state, an ASP Up Ack message is returned, as well as an Error message ("Unexpected Message), and the remote ASP state is changed to ASP-INACTIVE in all relevant Application Servers.

If an ASP Up message is received and internally the remote ASP is already in the ASP-INACTIVE state, an ASP Up Ack message is returned and no further action is taken.

4.3.4.1.1 SUA Version Control

If an ASP Up message with an unsupported version is received, the receiving end responds with an Error message, indicating the version the receiving node supports and notifies Layer Management.

This is useful when protocol version upgrades are being performed in a network. A node upgraded to a newer version should support the older versions used on other nodes it is communicating with. Because ASPs initiate the ASP Up procedure it is assumed that the Error message would normally come from the SGP.

4.3.4.1.2 IPSP Considerations

An IPSP may be considered in the ASP-INACTIVE state after and ASPUP or ASPUP Ack has been received from it. An IPSP can be considered in the ASP-DOWN state after an ASPDN or ASPDN Ack has been received from it. The IPSP may inform Layer Management of the change in state of the remote IPSP using M-ASP_UP or M-ASP_DN indication or confirmation primitives.

Alternatively, an interchange of ASPUP messages from each end can be performed. This option follows the ASP state transition diagram. It would need four messages for completion.

If for any local reason (e.g., management lock-out) and IPSP cannot respond to an ASP Up message with an ASP Up Ack message, it responds to an ASP Up message with an Error message with Reason "Refused - Management Blocking" and leaves the remote IPSP in the ASP-DOWN state.

4.3.4.2 ASP Down Procedures

The ASP will send an ASP Down message to an SGP when the ASP wishes to be removed from service in all Application Servers that it is a member and no longer receive any DATA, SSNM or ASPTM messages. This action MAY be initiated at the ASP by an M-ASP_DOWN request primitive

from Layer Management or MAY be initiated automatically by an SUA management function.

Whether the ASP is permanently removed from any AS is a function of configuration management. In the case where the ASP previously used the Registration procedures (see Section 4.4.1) to register within Application Servers but has not deregistered from all of them prior to sending the ASP Down message, the SGP MUST consider the ASP as Deregistered in all Application Servers that it is still a member.

The SGP marks the ASP as ASP-DOWN, informs Layer Management with an M-ASP_Down indication primitive, and returns an ASP Down Ack message to the ASP.

The SGP MUST send an ASP Down Ack message in response to a received ASP Down message from the ASP even if the ASP is already marked as ASP-DOWN at the SGP.

At the ASP, the ASP Down Ack message received is not acknowledged. Layer Management is informed with an M-ASP_DOWN confirm primitive. If the ASP receives an ASP Down Ack without having sent an ASP Down message, the ASP should now consider itself as in the ASP-DOWN state. If the ASP was previously in the ASP-ACTIVE or ASP_INACTIVE state, the ASP should then initiate procedures to return itself to its previous state.

When the ASP sends an ASP Down message it starts timer T(ack). If the ASP does not receive a response to an ASP Down message within T(ack), the ASP MAY restart T(ack) and resend ASP Down messages until it receives an ASP Down Ack message. T(ack) is provisionable, with a default of 2 seconds. Alternatively, retransmission of ASP Down messages MAY be put under control of Layer Management. In this method, expiry of T(ack) results in an M-ASP_DOWN confirm primitive carrying a negative indication.

4.3.4.3 ASP Active Procedures

Anytime after the ASP has received an ASP Up Ack message from the SGP or IPSP, the ASP MAY send an ASP Active message to the SGP indicating that the ASP is ready to start processing traffic. This action MAY be initiated at the ASP by an M-ASP_ACTIVE request primitive from Layer Management or MAY be initiated automatically by an SUA management function. In the case where an ASP wishes to process the traffic for more than one Application Server across a common SCTP association, the ASP Active message(s) SHOULD contain a list of one

or more Routing Contexts to indicate for which Application Servers the ASP Active message applies. It is not necessary for the ASP to include all Routing Contexts of interest in a single ASP Active message, thus requesting to become active in all Routing Contexts at the same time. Multiple ASP Active messages MAY be used to activate within the Application Servers independently, or in sets. In the case where an ASP Active message does not contain a Routing Context parameter, the receiver must know, via configuration data, which Application Server(s) the ASP is a member.

For the Application Servers that the ASP can successfully activate, the SGP or IPSP responds with one or more ASP Active Ack messages, including the associated Routing Context(s) and reflecting any Traffic Mode Type values present in the related ASP Active message. The Routing Context parameter MUST be included in the ASP Active Ack message(s) if the received ASP Active message contained any Routing Contexts. Depending on any Traffic Mode Type request in the ASP Active message or local configuration data if there is no request, the SGP moves the ASP to the correct ASP traffic state within the associated Application Server(s). Layer Management is informed with an M-ASP_Active indication. If the SGP or IPSP receives any Data messages before an ASP Active message is received, the SGP or IPSP MAY discard them. By sending an ASP Active Ack message, the SGP or IPSP is now ready to receive and send traffic for the related Routing

Context(s). The ASP SHOULD NOT send Data messages for the related Routing Context(s) before receiving an ASP Active Ack message, or it will risk message loss.

Multiple ASP Active Ack messages MAY be used in response to an ASP Active message containing multiple Routing Contexts, allowing the SGP or IPSP to independently acknowledge the ASP Active message for different (sets of) Routing Contexts. The SGP or IPSP MUST send an Error message ("Invalid Routing Context") for each Routing Context value that cannot be successfully activated.

In the case where an "out-of-the-blue" ASP Active message is received (i.e., the ASP has not registered with the SG or the SG has no static configuration data for the ASP), the message MAY be silently discarded.

The SGP MUST send an ASP Active Ack message in response to a received ASP Active message from the ASP, if the ASP is already marked in the ASP-ACTIVE state at the SGP.

At the ASP, the ASP Active Ack message received is not acknowledged. Layer Management is informed with an M-ASP_ACTIVE confirm primitive. It is possible for the ASP to receive Data message(s) before the ASP Active Ack message as the ASP Active Ack and Data messages from an SG or IPSP may be sent on different SCTP streams. Message loss is possible, as the ASP does not consider itself in the ASP-ACTIVE state until reception of the ASP Active Ack message.

When the ASP sends an ASP Active message it starts timer T(ack). If the ASP does not receive a response to an ASP Active message within T(ack), the ASP MAY restart T(ack) and resend ASP Active messages until it receives an ASP Active Ack message. T(ack) is provisionable, with a default of 2 seconds. Alternatively, retransmission of ASP Active messages MAY be put under control of Layer Management. In this method, expiry of T(ack) results in an M-ASP_ACTIVE confirm primitive carrying a negative indication.

There are three modes of Application Server traffic handling in the SGP SUA layer: Override, Load-share and Broadcast. When included, the Traffic Mode Type parameter in the ASP Active message indicates the traffic-handling mode to be used in a particular Application Server. If the SGP determines that the mode indicated in an ASP Active message is unsupported or incompatible with the mode currently configured for the AS, the SGP responds with an Error message ("Unsupported / Invalid Traffic Handling Mode"). If the traffic-handling mode of the Application Server is not already known via configuration data, then the traffic-handling mode indicated in the first ASP Active message causing the transition of the Application Server state to AS-ACTIVE MAY be used to set the mode.

In the case of an Override mode AS, reception of an ASP Active message at an SGP causes the (re)direction of all traffic for the AS to the ASP that sent the ASP Active message. Any previously active ASP in the AS is now considered to be in state ASP-INACTIVE and SHOULD no longer receive traffic from the SGP within the AS. The SGP or IPSP then MUST send a Notify message ("Alternate ASP Active") to the previously active ASP in the AS, and SHOULD stop traffic to/from that ASP. The ASP receiving this Notify MUST consider itself now in the ASP-INACTIVE state, if it is not already aware of this via inter-ASP communication with the Overriding ASP.

In the case of a Loadshare mode AS, reception of an ASP Active message at an SGP or IPSP causes the direction of traffic to the ASP sending the ASP Active message, in addition to all the other ASPs that are currently active in the AS. The algorithm at the SGP for load-sharing traffic within an AS to all the active ASPs is implementation dependent. The algorithm could, for example, be round robin or based on information in the Data message (e.g., the SLS or SSN).

An SGP or IPSP, upon reception of an ASP Active message for the first ASP in a Loadshare AS, MAY choose not to direct traffic to a newly active ASP until it determines that there are sufficient resources to handle the expected load (e.g., until there are "n" ASPs in state ASP-ACTIVE in the AS).

All ASPs within a load-sharing mode AS must be able to process any Data message received for the AS, to accommodate any potential fail-over or rebalancing of the offered load.

In the case of a Broadcast mode AS, reception of an ASP Active message at an SGP or IPSP causes the direction of traffic to the ASP sending the ASP Active message, in addition to all the other ASPs that are currently active in the AS. The algorithm at the SGP for broadcasting traffic within an AS to all the active ASPs is a simple broadcast algorithm, where every message is sent to each of the active ASPs. An SGP or IPSP, upon reception of an ASP Active message for the first ASP in a Broadcast AS, MAY choose not to direct traffic to a newly active ASP until it determines that there are sufficient resources to handle the expected load (e.g., until there are "n" ASPs in state ASP-ACTIVE in the AS).

Whenever an ASP in a Broadcast mode AS becomes ASP-ACTIVE, the SGP MUST tag the first DATA message broadcast in each SCTP stream with a unique Correlation Id parameter. The purpose of this Correlation Id is to permit the newly active ASP to synchronize it's processing of traffic in each ordered stream with the other ASPs in the broadcast group.

4.3.4.3.1 IPSP Consideratoins

Either of the IPSPs can initiate communication. When an IPSP receives an ASP Active, it should mark the peer as ASP-ACTIVE and return an ASP Active Ack message. An ASP receiving an ASP Active Ack message may mark the peer as ASP-Active, if it is not already in the ASP-ACTIVE state.

Alternatively, an interchange of ASPAC messages from each end can be performed. This option follows the ASP state transition diagram and gives the additional advantage of selecting a particular AS to be activated from each end. It is especially useful when an IPSP is serving more than one AS. It would need four messages for completion.

4.3.4.4 ASP Inactive Procedures

When an ASP wishes to withdraw from receiving traffic within an AS, the ASP sends an ASP Inactive message to the SGP or IPSP. This action MAY be initiated at the ASP by an M-ASP_INACTIVE request primitive from Layer Management or MAY be initiated automatically by an SUA management function. In the case where an ASP is processing the traffic for more than one Application Server across a common SCTP association, the ASP Inactive message contains one or more Routing Contexts to indicate for which Application Servers the ASP Inactive message applies. In the case where an ASP Inactive message does not contain a Routing Context parameter, the receiver must know, via configuration data, which Application Servers the ASP is a member and move the ASP to the ASP-INACTIVE state in each all Application Servers. In the case of an Override mode AS, where another ASP has already taken over the traffic within the AS with an ASP Active ("Override") message, the ASP that sends the ASP Inactive message is already considered by the SGP to be in state ASP-INACTIVE. An ASP

Inactive Ack message is sent to the ASP, after ensuring that all

traffic is stopped to the ASP.

In the case of a Load-share mode AS, the SGP moves the ASP to the ASP-INACTIVE state and the AS traffic is re-allocated across the remaining ASPs in the state ASP-ACTIVE, as per the load-sharing algorithm currently used within the AS. A Notify message ("Insufficient ASP resources active in AS") MAY be sent to all inactive ASPs, if required. An ASP Inactive Ack message is sent to the ASP after all traffic is halted and Layer Management is informed with an M-ASP_INACTIVE indication primitive.

In the case of a Broadcast mode AS, the SGP moves the ASP to the ASP-INACTIVE state and the AS traffic is broadcast only to the remaining ASPs in the state ASP-ACTIVE. A Notify message ("Insufficient ASP resources active in AS") MAY be sent to all inactive ASPs, if required. An ASP Inactive Ack message is sent to the ASP after all traffic is halted and Layer Management is informed with an M-ASP_INACTIVE indication primitive.

Multiple ASP Inactive Ack messages MAY be used in response to an ASP Inactive message containing multiple Routing Contexts, allowing the SGP or IPSP to independently acknowledge for different (sets of) Routing Contexts. The SGP or IPSP sends an Error message ("Invalid Routing Context") message for each invalid or unconfigured Routing Context value in a received ASP Inactive message.

The SGP MUST send an ASP Inactive Ack message in response to a received ASP Inactive message from the ASP and the ASP is already marked as ASP-INACTIVE at the SGP.

At the ASP, the ASP Inactive Ack message received is not acknowledged. Layer Management is informed with an M-ASP_INACTIVE confirm primitive. If the ASP receives an ASP Inactive Ack without having sent an ASP Inactive message, the ASP should now consider itself as in the ASP-INACTIVE state. If the ASP was previously in the ASP-ACTIVE state, the ASP should then initiate procedures to return itself to its previous state. When the ASP sends an ASP Inactive message it starts timer T(ack). If the ASP does not receive a response to an ASP Inactive message within T(ack), the ASP MAY restart T(ack) and resend ASP Inactive messages until it receives an ASP Inactive Ack message. T(ack) is provisionable, with a default of 2 seconds. Alternatively, retransmission of ASP Inactive messages MAY be put under control of Layer Management. In this method, expiry of T(ack) results in a M-ASP_Inactive confirm primitive carrying a negative indication.

If no other ASPs in the Application Server are in the state ASP-ACTIVE, the SGP MUST send a Notify message ("AS-Pending") to all of the ASPs in the AS which are in the state ASP-INACTIVE. The SGP SHOULD start buffering the incoming messages for T(r) seconds, after which messages MAY be discarded. T(r) is configurable by the network

operator. If the SGP receives an ASP Active message from an ASP in the AS before expiry of T(r), the buffered traffic is directed to that ASP and the timer is cancelled. If T(r) expires, the AS is moved to the AS-INACTIVE state.

4.3.4.4.1 IPSP Considerations

An IPSP may be considered in the ASP-INACTIVE state by a remote IPSP after an ASP Inactive or ASP Inactive Ack message has been received from it.

Alternatively, an interchange of ASPIA messages from each end can be performed. This option follows the ASP state transition diagram and gives the additional advantage of selecting a particular AS to be deactivated from each end. It is especially useful when an IPSP is serving more than one AS. It would need four messages for completion.

4.3.4.5 Notify Procedures

A Notify message reflecting a change in the AS state MUST be sent to all ASPs in the AS, except those in the ASP-DOWN state, withappropriate Status Information and any ASP Identifier of the failed ASP. At the ASP, Layer Management is informed with an M-NOTIFY indication primitive. The Notify message must be sent whether the AS state change was a result of an ASP failure or reception of an ASP State management (ASPSM) / ASP Traffic Management (ASPTM) message. In the second case, the Notify message MUST be sent after any ASP State or Traffic Management related acknowledgement messages (e.g., ASP Up Ack, ASP Down Ack, ASP Active Ack, or ASP Inactive Ack).

In the case where a Notify ("AS-PENDING") message is sent by an SGP that now has no ASPs active to service the traffic, or where a Notify ("Insufficient ASP resources active in AS") message MUST be sent in the Loadshare or Broadcast mode, the Notify message does not explicitly compel the ASP(s) receiving the message to become active. The ASPs remain in control of what (and when) traffic action is taken.

In the case where a Notify message does not contain a Routing Context parameter, the receiver must know, via configuration data, of which Application Servers the ASP is a member and take the appropriate action in each AS.

4.3.4.5.1 IPSP Considerations (NTFY)

Notify works in the same manner as in the SG-AS case. One of the IPSPs can send this message to any remote IPSP that is not in the ASP-DOWN state.

4.3.4.6 Heartbeat Procedures

The optional Heartbeat procedures MAY be used when operating over transport layers that do not have their own heartbeat mechanism for detecting loss of the transport association (i.e., other than SCTP).

Either SUA peer may optionally send Heartbeat messages periodically, subject to a provisionable timer T(beat). Upon receiving a Heartbeat message, the SUA peer MUST respond with a Heartbeat Ack message.

If no Heartbeat Ack message (or any other SUA message) is received from the SUA peer within 2*T(beat), the remote SUA peer is considered unavailable. Transmission of Heartbeat messages is stopped and the signalling process SHOULD attempt to re-establish communication if it is configured as the client for the disconnected SUA peer.

The Heartbeat message may optionally contain an opaque Heartbeat Data parameter that MUST be echoed back unchanged in the related Heartbeat Ack message. The sender, upon examining the contents of the returned Heartbeat Ack message, MAY choose to consider the remote SUA peer as unavailable. The contents/format of the Heartbeat Data parameter is implementation-dependent and only of local interest to the original sender. The contents may be used, for example, to support a Heartbeat sequence algorithm (to detect missing Heartbeats), and/or a timestamp mechanism (to evaluate delays).

Note: Heartbeat related events are not shown in Figure 4 "ASP state transition diagram".

4.4 Routing Key Management Procedures

4.4.1 Registration

An ASP MAY dynamically register with an SGP as an ASP within an Application Server using the REG REQ message. A Routing Key parameter in the REG REQ message specifies the parameters associated with the Routing Key.

The SGP examines the contents of the received Routing Key parameter and compares it with the currently provisioned Routing Keys. If the received Routing Key matches an existing SGP Routing Key entry, and the ASP is not currently included in the list of ASPs for the related Application Server, the SGP MAY authorize the ASP to be added to the AS. Or, if the Routing Key does not currently exist and the received Routing Key data is valid and unique, an SGP supporting dynamic configuration MAY authorize the creation of a new Routing Key and related Application Server and add the ASP to the new AS. In either case, the SGP returns a Registration Response message to the ASP, containing the same Local-RK-Identifier as provided in the initial request, and a Registration Result "Successfully Registered". A unique Routing Context value assigned to the SGP Routing Key is

included. The method of Routing Context value assignment at the SGP is implementation dependent but must be guaranteed to be unique for each Application Server or Routing Key supported by the SGP. If the SGP determines that the received Routing Key data is invalid, or contains invalid parameter values, the SGP returns a Registration Response message to the ASP, containing a Registration Result "Error - Invalid Routing Key", "Error - Invalid DPC", "Error - Invalid Network Appearance" as appropriate.

If the SGP does not support the registration procedure, the SGP returns an Error message to the ASP, with an error code of "Unsupported Message Type".

If the SGP determines that a unique Routing Key cannot be created, the SGP returns a Registration Response message to the ASP, with a Registration Status of "Error - "Cannot Support Unique Routing." An incoming signalling message received at an SGP should not match against more than one Routing Key.

If the SGP does not authorize the registration request, the SGP returns a REG RSP message to the ASP containing the Registration Result "Error - Permission Denied".

If an SGP determines that a received Routing Key does not currently exist and the SGP does not support dynamic configuration, the SGP returns a Registration Response message to the ASP, containing a Registration Result "Error - Routing Key not Currently Provisioned".

If an SGP determines that a received Routing Key does not currently exist and the SGP supports dynamic configuration but does not have the capacity to add new Routing Key and Application Server entries, the SGP returns a Registration Response message to the ASP, containing a Registration Result "Error - Insufficient Resources".

If an SGP determines that one or more of the Routing Key parameters are not supported for the purpose of creating new Routing Key entries, the SGP returns a Registration Response message to the ASP, containing a Registration Result "Error - Unsupported RK parameter field". This result MAY be used if, for example, the SGP does not support RK Address parameter.

A Registration Response "Error - Unsupported Traffic Handling Mode" is returned if the Routing Key in the REG REQ contains a Traffic Handling Mode that is inconsistent with the presently configured mode for the matching Application Server.

An ASP MAY register multiple Routing Keys at once by including a number of Routing Key parameters in a single REG REQ message. The SGP MAY respond to each registration request in a single REG RSP message, indicating the success or failure result for each Routing Key in a separate Registration Result parameter. Alternatively the SGP MAY respond with multiple REG RSP messages, each with one or more

Registration Result parameters. The ASP uses the Local-RK-Identifier parameter to correlate the requests with the responses.

An ASP MAY modify an existing Routing Key by including a Routing Context parameter in the REG REQ. If the SGP determines that the Routing Context applies to an existing Routing Key, the SG MAY adjust the existing Routing Key to match the new information provided in the Routing Key parameter. A Registration Response "Routing Context Registionation Refused" is returned if the SGP does not accept the modification of the Routing Key.

Upon successful registration of an ASP in an AS, the SGP can now send related SS7 Signalling Network Management messaging, if this did not previously start upon the ASP transitioning to state ASP-INACTIVE

4.4.2 Deregistration

An ASP MAY dynamically deregister with an SGP as an ASP within an Application Server using the DEREG REQ message. A Routing Context parameter in the DEREG REQ message specifies which Routing Keys to de-register. An ASP SHOULD move to the ASP-INACTIVE state for an Application Server before attempting to deregister the Routing Key (i.e., deregister after receiving an ASP Inactive Ack). Also, an ASP SHOULD deregister from all Application Servers that it is a member before attempting to move to the ASP-Down state.

The SGP examines the contents of the received Routing Context parameter and validates that the ASP is currently registered in the Application Server(s) related to the included Routing Context(s). If validated, the ASP is de-registered as an ASP in the related Application Server.

The deregistration procedure does not necessarily imply the deletion ofRouting Key and Application Server configuration data at the SGP. Other ASPs may continue to be associated with the Application Server, in which case the Routing Key data SHOULD NOT be deleted. If a Deregistration results in no more ASPs in an Application Server, an SGP MAY delete the Routing Key data.

The SGP acknowledges the deregistration request by returning a DEREG RSP message to the requesting ASP. The result of the deregistration is found in the Deregistration Result parameter, indicating success or failure with cause.

An ASP MAY deregister multiple Routing Contexts at once by including a number of Routing Contexts in a single DEREG REQ message. The SGP MAY respond to each deregistration request in a single DEREG RSP message, indicating the success or failure result for each Routing Context in a separate Deregistration Result parameter.

4.4.3 IPSP Considerations (REG/DEREG)

The Registration/Deregistration procedures work in the IPSP cases in the same way as in AS-SG cases. An IPSP may register an RK in the remote IPSP. An IPSP is responsible for deregistering the RKs that it has registered.

4.5 Availability and/or Congestion Status of SS7 Destination Support

4.5.1 At an SGP

On receiving a N-STATE, N-PCSTATE and N-INFORM indication primitive from the nodal inter-working function at an SGP, the SGP SUA layer will send a corresponding SS7 Signalling Network Management (SSNM) DUNA, DAVA, SCON, or DUPU message (see Section 3.4) to the SUA peers at concerned ASPs. The SUA layer must fill in various fields of the

SSNM messages consistently with the information received in the primitives.

The SGP SUA layer determines the set of concerned ASPs to be informed based on the specific SS7 network for which the primitive indication is relevant. In this way, all ASPs configured to send/receive traffic within a particular network appearance are informed. If the SGP operates within a single SS7 network appearance, then all ASPs are informed.

DUNA, DAVA, SCON, and DRST messages are sent sequentially and processed at the receiver in the order sent. SCTP stream 0 SHOULD NOT be used. The Unordered bit in the SCTP DATA chunk MAY be used for the SCON message.

Sequencing is not required for the DUPU or DAUD messages, which MAY be sent un-sequenced. Again, SCTP stream 0 is used, with optional use of the Unordered bit in the SCTP DATA chunk.

4.5.2 At an ASP

4.5.2.1 Single SG Configurations

At an ASP, upon receiving an SS7 Signalling Network Management (SSNM) message from the remote SUA Peer, the SUA layer invokes the appropriate primitive indications to the resident SUA-Users. Local management is informed.

In the case where a local event has caused the unavailability or congestion status of SS7 destinations, the SUA layer at the ASP SHOULD pass up appropriate indications in the primitives to the SUA User, as though equivalent SSNM messages were received. For example, the loss of an SCTP association to an SGP may cause the unavailability of a set of SS7 destinations. N-PCSTATE indication primitives to the SUA User are appropriate.

Implementation Note: To accomplish this, the SUA layer at an ASP maintains the status of routes via the SG.

4.5.2.2 Multiple SG Configurations

At an ASP, upon receiving a Signalling Network Management message from the remote SUA Peer, the SUA layer updates the status of the affected route(s) via the originating SG and determines, whether or not the overall availability or congestion status of the effected destination(s) has changed. If so, the SUA layer invokes the appropriate primitive indications to the resident SUA-Users. Local management is informed.

4.5.3 ASP Auditing

An ASP may optionally initiate an audit procedure to enquire of an SGP the availability and, if the national congestion method with multiple congestion levels and message priorities is used, congestion status of an SS7 destination or set of destinations. A Destination Audit (DAUD) message is sent from the ASP to the SGP requesting the current availability and congestion status of one or more SS7 destinations or subsystems.

The DAUD message MAY be sent un-sequenced. The ASP MAY send the DAUD in the following cases:

- Periodic. A Timer originally set upon reception of a DUNA, SCON or DRST message has expired without a subsequent DAVA, DUNA, SCON or DRST message updating the availability/congestion status of the affected Destination Point Code. The Timer is reset upon issuing a DAUD. In this case the DAUD is sent to

the SGP that originally sent the SSNM message.

- Isolation. The ASP is newly ASP-ACTIVE or has been isolated from an SGP for an extended period. The ASP MAY request the availability/congestion status of one or more SS7 destinations to which it expects to communicate.

Implementation Note:

In the first of the cases above, the auditing procedure must not be invoked for the case of a received SCON message containing a congestion level value of "no congestion" or undefined" (i.e., congestion Level = "0"). This is because the value indicates either congestion abatement or that the ITU MTP3 international congestion method is being used. In the international congestion method, the MTP3 layer at the SGP does not maintain the congestion status of any destinations and therefore the SGP cannot provide any congestion information in response to the DAUD. For the same

reason, in the second of the cases above a DAUD message cannot reveal any congested destination(s).

The SGP SHOULD respond to a DAUD message with the availability and congestion status of the subsystem. The status of each SS7 destination or subsystem requested is indicated in a DUNA message (if unavailable), a DAVA message (if available), or a DRST (if restricted and the SGP supports this feature). If the SS7 destination or subsystem is available and congested, the SGP responds with an SCON message in addition to the DAVA message. If the SS7 destination or subsystem is restricted and congested, the SGP responds with an SCON message in addition to the DRST. If the SGP has no information on the availability / congestion status of the SS7 destination or subsystem, the SGP responds with a DUNA message, as it has no routing information to allow it to route traffic to this destination or subsystem.

An SG MAY refuse to provide the availability or congestion status of a destination or subsystem if, for example, the ASP is not authorized to know the status of the destination or subsystem. The SG MAY respond with an Error Message (Error Code = "Destination Status Unknown") or Error Message (Error Code = "Subsystem Status Unknown").

4.6 MTP3 Restart

In the case where the MTP3 in the SG undergoes an MTP restart, event communication SHOULD be handled as follows:

When the SG discovers SS7 network isolation, the SGPs send an indication to all concerned available ASPs (i.e., ASPs in the ASP-ACTIVE state) using DUNA messages for the concerned destinations. When the SG has completed the MTP Restart procedure, the SUA layer at the SGPs inform all concerned ASPs in the ASP-ACTIVE state of any available/restricted SS7 destinations using the DAVA/DRST message. No message is necessary for those destinations still unavailable after the restart procedure.

When the SUA layer at an ASP receives a DUNA message indicating SS7 destination unavailability at an SG, Users will stop any affected traffic to this destination. When the SUA layer receives a DAVA/DRST message, Users can resume traffic to the newly available SS7 destination via this SGP, provided the ASP is in the ASP-ACTIVE state towards this SGP.

The ASP MAY choose to audit the availability of unavailable destinations by sending DAUD messages. This would be for example the case when an AS becomes active at an ASP and does not have up to date destination statuses. If MTP restart is then in progress at the SG, the SGP returns a DUNA message for that destination, even if it received an indication that the destination became available or

restricted.

4.7 SCCP - SUA Interworking at the SG

4.7.1 Segmenting / Reassembly

When it is expected that signalling messages will not fit into a PDU of the most restrictive transport technology used (e.g. 272-SIF of MTP3), then segmenting/reassembly could be performed at the SG, ASP or IPSP. If the SG, ASP or IPSP is incapable of performing a necessary segmentation/reassembly, it can inform the peer of the failure using the appropriate error in a CLDR or RESRE/COERR message.

4.7.2 Support for Loadsharing

Within an AS (identified by RK/RC parameters) several loadsharing ASPs may be active.

However, in order to assure the correct processing of TCAP transactions or SCCP connections, the loadsharing scheme used at the SG must make sure that messages continuing or ending the ransactions/connections arrive at the same ASP where the initial message (TC_Query, TC_Begin, CR) was sent to/received from.

When the ASP can be identified uniquely based on RK parameters (e.g. unique DPC or GT), loadsharing is not required. When the ASPs in the AS share state or use an internal distribution mechanism, the SG must only take into account the in-sequence-delivery requirement. In case of SCCP CO traffic, when the coupled approach is used, loadsharing of messages other than CR is not required.

If these assumptions cannot be made, both SG and ASP should support the following general procedure in a loadsharing environment.

4.7.2.1 Association Setup, ASP going active

After association setup and registration, an ASP normally goes active for each AS it registered for. In the ASPAC message, the ASP includes a TID and/or DRN Label Parameter, if applicable for the AS in question. All the ASPs within the AS must specify a unique label at a fixed position in the TID or DRN parameter. The same ASPAC message is sent to each SG used for interworking with the SS7 network.

The SG builds, per RK, a list of ASPs that have registered for it. The SG can now build up and update a distribution table for a certain Routing Context, any time the association is (re-)established and the ASP goes active. The SG has to perform some trivial plausibility checks on the parameters:

- Start and End parameters values are between 0 and 31 for TID.
- Start and End parameters values are between 0 and 23 for DRN
- 0 < (Start - End + 1) <= 16 (label length maximum 16-bit)
- Start values are the same for each ASP within a RC

- End values are the same for each ASP within a RC
- TID and DRN Label values must be unique across the RC

If any of these checks fail, the SG refuses the ASPAC request, with an error, "Invalid loadsharing label."

4.7.3 Routing and message distribution at the SG

4.7.3.1 TCAP traffic

Messages not containing a destination (or "responding") TID, i.e. Query, Begin, Unidirectional, are loadshared among the available ASPs. Any scheme permitting a fair load distribution among the ASPs is allowed (e.g. round robin).

When a destination TID is present, the SG extracts the label and selects the ASP that corresponds with it.

If an ASP is not available, the SG may generate (X)UDTS "routing failure", if the return option is used.

4.7.3.2 SCCP Connection Oriented traffic

Messages not containing a destination reference number (DRN), i.e. a Connection Request, MAY be loadshared among the available ASPs. The load distribution mechanism is an implementation issue. When a DRN is present, the SG extracts the label and selects the ASP that corresponds with it. If an ASP is not available, the SG discards the message.

4.7.4 Multiple SGs, SUA Relay Function

It is important that each ASP send its unique label (within the AS) to each SGP. For a better robustness against association failures, the SGs MAY cooperate to provide alternative routes towards an ASP. Mechanisms for SG cooperation/co-ordination are outside of the scope of this document.

5 Examples of SUA Procedures

The following sequence charts overview the procedures of SUA. These are meant as examples, they do not, in and of themselves, impose additional requirements upon an instance of SUA.

5.1 SG Architecture

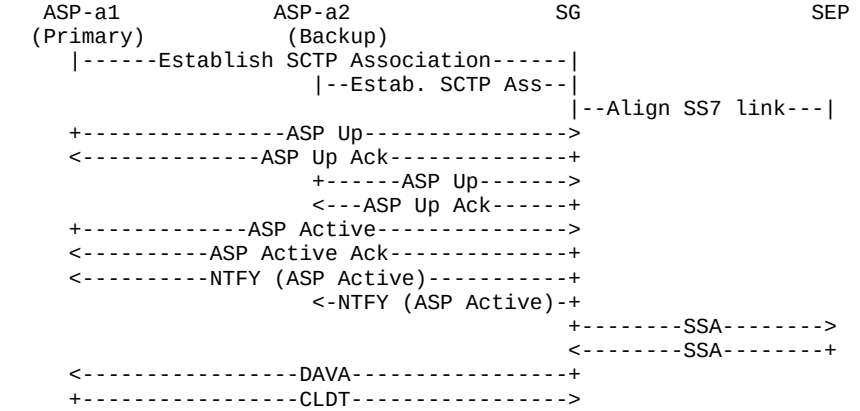
The sequences below outline logical steps for a variety of scenarios within a SG architecture. Please note that these scenarios cover a Primary/Backup configuration. Where there is a load-sharing configuration then the SGP can declare availability when 1 ASP

issues ASPAC but can only declare unavailability when all ASPs have issued ASPIA.

5.1.1 Establishment of SUA connectivity

The following is established before traffic can flow.

Each node is configured (via MIB, for example) with the connections that need to be setup.



```
                                                +--------UDT-------->
```

5.1.2 Failover scenarios

The following sequences address failover of SEP and ASP

5.1.2.1 SEP Failover

The SEP knows that the SGP is 'concerned' about its availability. Similarly, the SGP knows that ASP-a1 is concerned about the SEPs availability.

```
     ASP-a1            ASP-a2               SG                  SEP
   (Primary)           (Backup)
                                             <--------SSP--------+
       <-----------------DUNA-----------------+
       +-----------------DAUD----------------->
                                             +--------SST-------->
```

5.1.2.2 Successful ASP Failover scenario

The following is an example of a successful failover scenario, where there is a failover from ASP-a1 to ASP-a2, i.e. Primary to Backup. During the failover, the SGP buffers any incoming data messages from the SEP, forwarding them when the Backup becomes available.


```
     ASP-a1            ASP-a2               SG                  SEP
   (Primary)           (Backup)
       +-------------ASP Inactive------------>
       <-----------ASP Inactive ACK-----------+
       <--------------------NTFY (AS Pending)-+
                          <-NTFY (AS Pending)-+
                          +----ASP Active----->
                          <--ASP Active Ack---+
                          <-NTFY (AS Active)--+
       <----------NTFY (AS Active)------------+
```

5.1.2.3 Unsuccessful ASP Failover scenario

```
     ASP-a1            ASP-a2               SG                  SEP
   (Primary)           (Backup)
       +-------------ASP Inactive------------>
       <-----------ASP Inactive ACK-----------+
       <--------------------NTFY (AS Pending)-+
                        <--NTFY (AS Pending)-+
             After some time elapses (i.e. timeout).
                                             +--------SSP-------->
                                             <--------SST--------+
       <-------------------NTFY (AS Inactive)-+
                         <-NTFY (AS Inactive)-+
```

5.2 IPSP Examples.

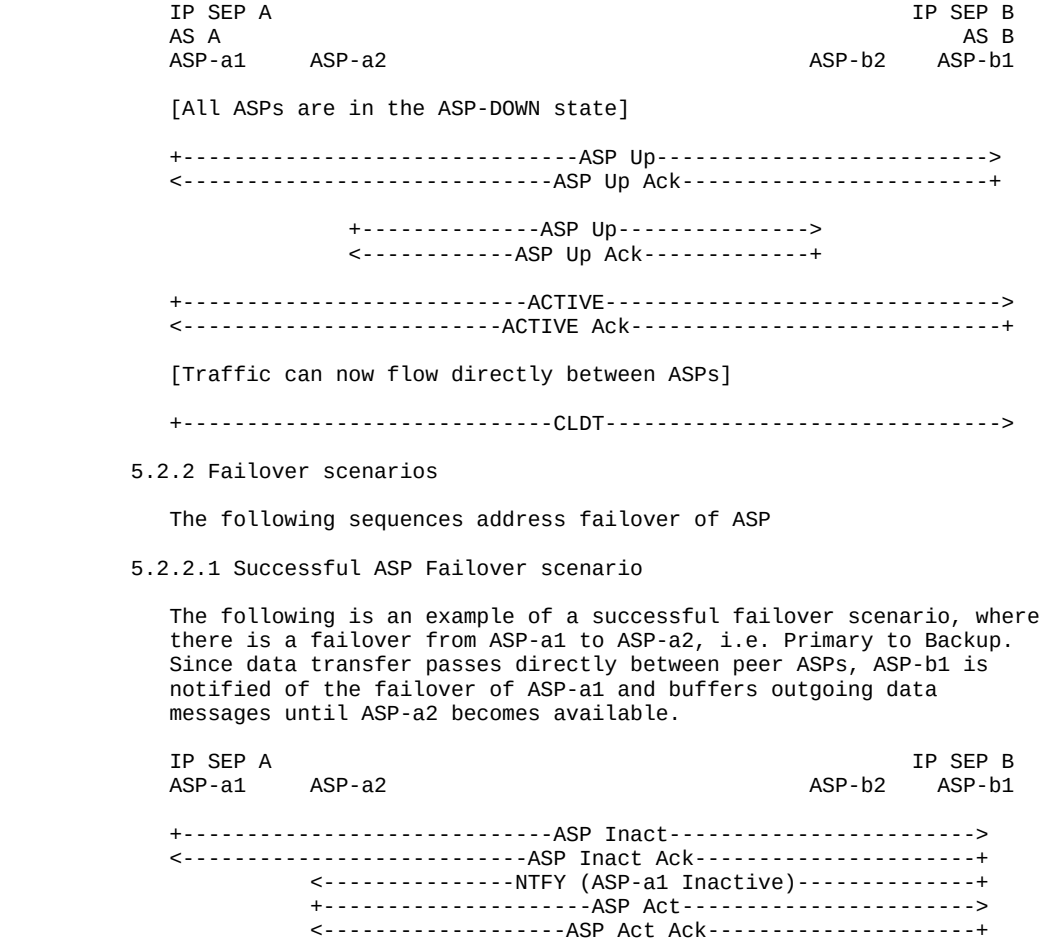
The sequences below outline logical steps for a variety of scenarios within an IP-IP architecture. Please note that these scenarios cover a Primary/Backup configuration. Where there is a load-sharing configuration then the AS can declare availability when 1 ASP issues ASPAC but can only declare unavailability when all ASPs have issued ASPIA.

5.2.1 Establishment of SUA connectivity

The following shows an example establishment of SUA connectivity. In this example, each IPSP consists of an Application Server and two ASPs. The following is established before SUA traffic can flow. A connectionless flow is shown for simplicity.

Establish SCTP Connectivity - as per RFC 2960. Note that SCTP connections are bi-directional. The endpoint that establishes SCTP connectivity MUST also establishes UA connectivity (see RFC 2960,

section 5.2.1 for handling collisions) [2960].



5.2.2 Failover scenarios

The following sequences address failover of ASP

5.2.2.1 Successful ASP Failover scenario

The following is an example of a successful failover scenario, where there is a failover from ASP-a1 to ASP-a2, i.e. Primary to Backup. Since data transfer passes directly between peer ASPs, ASP-b1 is notified of the failover of ASP-a1 and buffers outgoing data messages until ASP-a2 becomes available.

5.2.2.2 Unsuccessful ASP Failover scenario

The sequence is the same as 5.2.2.1 except that, since the backup fails to come in then, the Notify messages declaring the availability of the backup are not sent.

6 Security Considerations

6.1 Introduction

SUA is designed to carry signaling messages for telephony services. In some cases, SUA may be deployed on both an intra-domain (single service provider) and an inter-domain (multiple service providers) basis. The security requirements for these situations may be

different.

SUA involves the security needs of several parties: the end users of the services; the network providers and the applications involved. Additional security requirements may come from local regulation. While having some overlapping security needs, any security solution should fulfill all of the different parties' needs.

SUA assumes that messages are secured by using either IPSec or TLS.

6.2 Threats

There is no quick fix, one-size-fits-all solution for security. As a transport protocol, SUA has the following security objectives:

* Availability of reliable and timely user data transport.
* Integrity of user data transport.
* Confidentiality of user data.

SUA runs on top of SCTP. SCTP provides certain transport related security features, such as:

* Blind Denial of Service Attacks
* Flooding
* Masquerade
* Improper Monopolization of Services

When SUA is running in professionally managed corporate or service provider network, it is reasonable to expect that this network include an appropriate security policy framework. The "Site Security Handbook" [2196] should be consulted for guidance.

SS7 networks have a different security model than IP networks. Traditionally, the PSTN has been a private and closed network, where in many cases, in order to get connectivity, one would need to be a service provider and negotiate physical connections to the PSTN.

The Internet has a slightly different security model, one which connectivity is a primary goal. When signaling protols are run over IP, one must be aware that it is impossible to guarantee that the IP network will be physically separate from another IP network. Firewalls and gateways may create an illusion of separateness, but do not guarentee this. One misconfigured parameter in a firewall could leave a dangerous security hole.

The most reasonable security model for SUA is to assume a virtual private network (VPN) type of security, where TLS or IPsec are used to encrypt traffic between nodes.

6.3 Protecting Confidentiality

Particularly for mobile users, the requirement for confidentiality may include the masking of IP addresses and ports. In this case application level encryption is not sufficient; IPSEC ESP should be used instead. Regardless of which level performs the encryption, the IPSEC ISAKMP service should be used for key management.

6.4 IPsec Usage

All SUA implementations MUST support IPsec ESP [IPsec] in transport mode with with non-null encryption and authentication algorithms to provide per-packet authentication, integrity protection and confidentiality, and MUST support the replay protection mechanisms of IPsec.

SUA implementations MUST support IKE for peer authentication, negotiation of security associations, and key management, using the IPsec DOI [IPSECDOI]. SUA implementations MUST support peer authentication using a pre-shared key, and MAY support certificate-based peer authentication using digital signatures. Peer

authentication using the public key encryption methods outlined in IKE's sections 5.2 and 5.3 [IKE] SHOULD NOT be used.

Conformant implementations MUST support both IKE Main Mode and Aggressive Mode. When pre-shared keys are used for authentication, IKE Aggressive Mode SHOULD be used, and IKE Main Mode SHOULD NOT be used. When digital signatures are used for authentication, either IKE Main Mode or IKE Aggressive Mode MAY be used.

When digital signatures are used to achieve authentication, an IKE negotiator SHOULD use IKE Certificate Request Payload(s) to specify the certificate authority (or authorities) that are trusted in accordance with its local policy. IKE negotiators SHOULD use pertinent certificate revocation checks before accepting a PKI certificate for use in IKE's authentication procedures.

The Phase 2 Quick Mode exchanges used to negotiate protection for SUA connections MUST explicitly carry the Identity Payload fields (IDci and IDcr). The DOI provides for several types of identification data. However, when used in conformant implementations, each ID Payload MUST carry a single IP address and a single non-zero port number, and MUST NOT use the IP Subnet or IP Address Range formats. This allows the Phase 2 security association to correspond to specific TCP and SCTP connections.

Since IPsec acceleration hardware may only be able to handle a limited number of active IKE Phase 2 SAs, Phase 2 delete messages may be sent for idle SAs, as a means of keeping the number of active Phase 2 SAs to a minimum. The receipt of an IKE Phase 2 delete message SHOULD NOT be interpreted as a reason for tearing down a SUA

connection. Rather, it is preferable to leave the connection up, and if additional traffic is sent on it, to bring up another IKE Phase 2 SA to protect it. This avoids the potential for continually bringing connections up and down.

6.5 TLS Usage

A SUA peer that initiates a connection to another SUA peer acts as a TLS client according to [TLS], and a SUA peer that accepts a connection acts as a TLS server. SUA peers implementing TLS for security MUST mutually authenticate as part of TLS session establishment. In order to ensure mutual authentication, the SUA node acting as TLS server must request a certificate from the SUA node acting as TLS client, and the SUA node acting as TLS client MUST be prepared to supply a certificate on request.

SUA peers supporting TLS MUST be able to negotiate the following TLS cipher suites:

```
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
```

SUA nodes MAY negotiate other TLS cipher suites.

6.6 Peer-to-Peer Considerations

As with any peer-to-peer protocol, proper configuration of the trust model within a SUA peer is essential to security. When certificates are used, it is necessary to configure the root certificate authorities trusted by the SUA peer. These root CAs are likely to be unique to SUA usage and distinct from the root CAs that might be trusted for other purposes such as Web browsing. In general, it is expected that those root CAs will be configured so as to reflect the business relationships between the organization hosting the SUA peer and other organizations. As a result, a SUA peer will typically not be configured to allow connectivity with any arbitrary peer. When certificate authentication SUA peers may not be known beforehand, and therefore peer discovery may be required.

Note that IPsec is considerably less flexible than TLS when it comes to configuring root CAs. Since use of Port identifiers is prohibited within IKE Phase 1, within IPsec it is not possible to uniquely configure trusted root CAs for each application individually; the same policy must be used for all applications. This implies, for example, that a root CA trusted for use with SUA must also be trusted to protect SNMP. These restrictions can be awkward at best. Since TLS supports application-level granularity in certificate policy, TLS SHOULD be used to protect SUA connections between administrative domains. IPsec is most appropriate for intra-domain usage when pre-shared keys are used as a security mechanism.

When pre-shared key authentication is used with IPsec to protect SUA, unique pre-shared keys are configured with SUA peers, who are identified by their IP address (Main Mode), or possibly their FQDN (Aggressive Mode). As a result, it is necessary for the set of SUA peers to be known beforehand. Therefore, peer discovery is typically not necessary.

The following is intended to provide some guidance on the issue.

It is recommended that a SUA peer implement the same security mechanism (IPsec or TLS) across all its peer-to-peer connections. Inconsistent use of security mechanisms can result in redundant security mechanisms being used (e.g. TLS over IPsec) or worse, potential security vulnerabilities. When IPsec is used with SUA, a typical security policy for outbound traffic is "Initiate IPsec, from me to any, destination port SUA"; for inbound traffic, the policy would be "Require IPsec, from any to me, destination port SUA".

This policy causes IPsec to be used whenever a SUA peer initiates a connection to another SUA peer, and to be required whenever an inbound SUA connection occurs. This policy is attractive, since it does not require policy to be set for each peer or dynamically modified each time a new SUA connection is created; an IPsec SA is automatically created based on a simple static policy. Since IPsec extensions are typically not available to the sockets API on most platforms, and IPsec policy functionality is implementation dependent, use of a simple static policy is the often the simplest route to IPsec-enabling a SUA implementation.

One implication of the recommended policy is that if a node is using both TLS and IPsec, there is not a convenient way in which to use either TLS or IPsec, but not both, without reserving an additional port for TLS usage. Since SUA uses the same port for TLS and non-TLS usage, where the recommended IPsec policy is put in place, a TLS-protected connection will match the IPsec policy, and both IPsec and TLS will be used to protect the SUA connection. To avoid this, it would be necessary to plumb peer-specific policies either statically or dynamically.

If IPsec is used to secure SUA peer-to-peer connections, IPsec policy SHOULD be set so as to require IPsec protection for inbound connections, and to initiate IPsec protection for outbound connections. This can be accomplished via use of inbound and outbound filter policy.

7 IANA Considerations

7.1 SCTP Payload Protocol ID

IANA has assigned a SUA value for the Payload Protocol Identifier in the SCTP DATA chunk. The following SCTP Payload Protocol Identifier is registered:

SUA "4"

The SCTP Payload Protocol Identifier value "4" SHOULD be included in each SCTP DATA chunk, to indicate that the SCTP is carrying the SUA protocol. The value "0" (unspecified) is also allowed but any other values MUST not be used. This Payload Protocol Identifier is not directly used by SCTP but MAY be used by certain network entities to identify the type of information being carried in a DATA chunk.

The User Adaptation peer MAY use the Payload Protocol Identifier, as a way of determining additional information about the data being presented to it by SCTP.

7.2 Port Number

IANA has registered SCTP Port Number 14001 for SUA. It is recommended that SGPs use this SCTP port number for listening for new connections. SGPs MAY also use statically configured SCTP port numbers instead.

7.3 Protocol Extensions

This protocol may also be extended through IANA in three ways:

- Through definition of additional message classes.
- Through definition of additional message types.
- Through definition of additional message parameters.

The definition and use of new message classes, types and parameters is an integral part of SIGTRAN adaptation layers. Thus, these extensions are assigned by IANA through an IETF Consensus action as defined in [RFC2434].

The proposed extension MUST in no way adversely affect the general working of the protocol.

A new registry will be created by IANA to allow the protocol to be extended

7.3.1 IETF Defined Message Classes

The documentation for a new message class MUST include the following information:
(a) A long and short name for the message class;
(b) A detailed description of the purpose of the message class.

7.3.2 IETF Defined Message Types

Documentation of the message type MUST contain the following information:

(a) A long and short name for the new message type;
(b) A detailed description of the structure of the message.
(c) A detailed definition and description of intended use of each field within the message.
(d) A detailed procedural description of the use of the new message type within the operation of the protocol.
(e) A detailed description of error conditions when receiving this message type.

When an implementation receives a message type which it does not support, it MUST respond with an Error (ERR) message, with an Error Code = Unsupported Message Type.

7.3.4 IETF-defined TLV Parameter Extension

Documentation of the message parameter MUST contain the following information:

(a) Name of the parameter type.
(b) Detailed description of the structure of the parameter field. This structure MUST conform to the general type-length-value format described earlier in the document.
(c) Detailed definition of each component of the parameter value.
(d) Detailed description of the intended use of this parameter type, and an indication of whether and under what circumstances multiple instances of this parameter type may be found within the same message type.

8 Timer Values

Ta		2 seconds
Tr		2 seconds
T(ack)		2 seconds
T(ias)	Inactivity Send timer	7 minutes
T(iar)	Inactivity Receive timer	15 minutes
T(beat)	Heartbeat Timer	30 seconds

9 Acknowledgements

The authors would like to thank (in alphabetical order) Javier Pastor-Balbas, Andrew Booth, Martin Booyens, F. Escobar, S. Furniss Klaus Gradischnig, Miguel A. Garcia, Marja-Liisa Hamalainen, Sherry Karl, S. Lorusso, Markus Maanoja, Sandeep Mahajan, Ken Morneault, Guy Mousseau, Chirayu Patel, Michael Purcell, W. Sully, Michael Tuexen, Al Varney, Tim Vetter, Antonio Villena, Ben Wilson, Michael Wright and James Yu for their insightful comments and suggestions.

10 Authors' Addresses

John Loughney
Nokia Research Center
PO Box 407
FIN-00045 Nokia Group
Finland
EMail: john.Loughney@nokia.com

Greg Sidebottom
gregside consulting
Kanata, Ontario
Canada
EMail: gregside@home.com

Lode Coene
Siemens Atea
Atealaan 34
B-2200 Herentals
Belgium
Phone: +32-14-252081
EMail: lode.coene@siemens.atea.be

Gery Verwimp
Siemens Atea
34 Atealaan
PO 2200
Herentals
Belgium
Phone: +32 14 25 3424
EMail: gery.verwimp@siemens.atea.be

Joe Keller

Tekelec
5200 Paramount Parkway
Morrisville, NC 27560
USA
EMail: joe.keller@tekelec.com

Brian Bidulock
OpenSS7 Corporation
4701 Preston Park Boulevard
Suite 424
Plano TX 75093
USA
EMail: bidulock@openss7.org

11 References

11.1 Normative

[1123] RFC 1123, "Requirements for Internet Hosts -- Application and Support" Braden, R. (Editor), October 1989.

[2196] RFC 2196, "Site Security Handbook", B. Fraser Ed., September 1997.

[2279] RFC 2279, "UTF-8, a transformation format of ISO 10646", January 1998.

[2401] RFC 2401, "Security Architecture for the Internet Protocol", S. Kent, R. Atkinson, November 1998.

[2960] RFC 2960 "Stream Control Transport Protocol" R. Stewart, et al, November 2000.

[ANSI SCCP] ANSI T1.112 'Signalling System Number 7 - Signalling Connection Control Part'

[IKE] D. Harkins, D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.

[IPSECDOI] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.

[ITU SCCP] ITU-T Recommendations Q.711-714, 'Signalling System No. 7 (SS7) - Signalling Connection Control Part (SCCP)'

[TLS] T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[TLSSCTP] M. Tuexen, et al. "TLS over SCTP" IETF Work in Progress.

11.2 Non-Normative

[2434] RFC 2434, "Guidelines for Writing an IANA Considerations Section in RFCs", T. Narten, H. Alvestrand, October 1998.

[2719] RFC 2719, "Framework Architecture for Signaling Transport"

[2916] RFC 2916, "E.164 number and DNS", P. Faltstrom, September 2000.

[ANSI-MTP] ANSI T1.111 'Signalling System Number 7 - Message Transfer Part'

[ANSI TCAP] ANSI T1.114 'Signalling System Number 7 - Transaction Capabilities Application Part'

[ITU-MTP] ITU-T Recommendations Q.701-Q.705, 'Signalling System No. 7 (SS7) - Message Transfer Part (MTP)'

[ITU TCAP] ITU-T Recommendation Q.771-775 'Signalling System No. 7 SS7) - Transaction Capabilities (TCAP)

[M3UA] MTP3-User Adaptation Layer, Work in Progress.

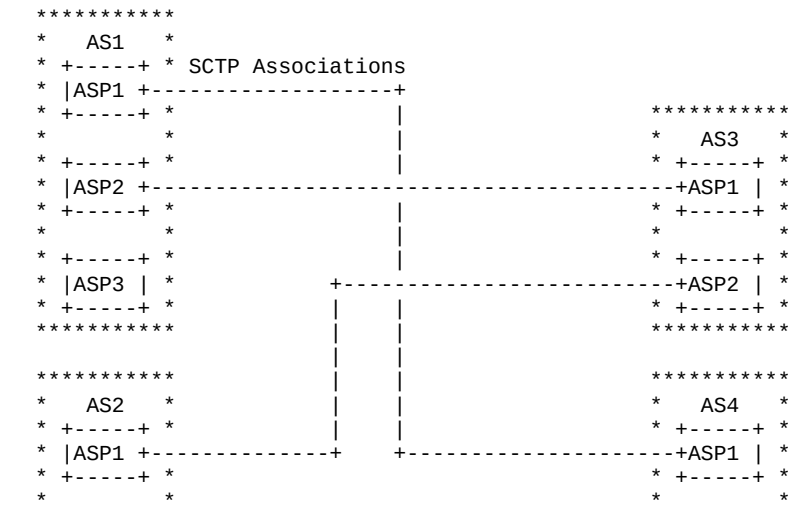
[RANAP] 3G TS 25.413 V3.5.0 (2001-03) 'Technical Specification 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu Interface RANAP Signalling'

[UTRAN IUR] 3G TS 25.422 V3.5.0 (2000-12) "Technical Specification 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iur Interface Signalling Transport (Release 1999)"

Appendix A Signaling Network Architecture

A.1 Generalized Peer-to-Peer Network Architecture

Figure 1 shows an example network architecture that can support robust operation and failover. There need to be some management resources at the AS to manage traffic.



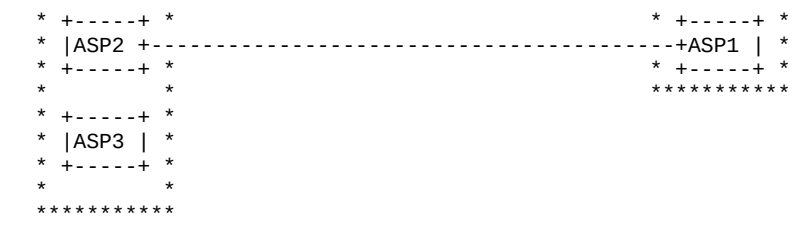


Figure 1: Generalized Architecture

In this example, the Application Servers are shown residing within one logical box, with ASPs located inside. In fact, an AS could be distributed among several hosts. In such a scenario, the host should share state as protection in the case of a failure. This is out of scope of this protocol. Additionally, in a distributed system, one ASP could be registered to more than one AS. This draft should not restrict such systems - though such a case in not specified.

A.2 Signalling Gateway Network Architecture

When interworking between SS7 and IP domains is needed, the SGP acts as the gateway node between the SS7 network and the IP network. The SGP will transport SCCP-user signalling traffic from the SS7 network to the IP-based signalling nodes (for example IP-resident Databases). The Signalling Gateway can be considered as a group of Application Servers with additional functionality to interface towards an SS7 network.

The SUA protocol should be flexible enough to allow different configurations and transport technology to allow the network operators to meet their operation, management and performance requirements.

An ASP may be connected to multiple SGPs (see figure 2). In such a case, a particular SS7 destination may be reachable via more than SG, therefore, more than one route. Given that proper SLS selection, loadsharing, and SG selection based on point code availability is performed at the ASP, it will be necessary for the ASP to maintain the status of each distant SGPs to which it communicates on the basis of the SG through which it may route.

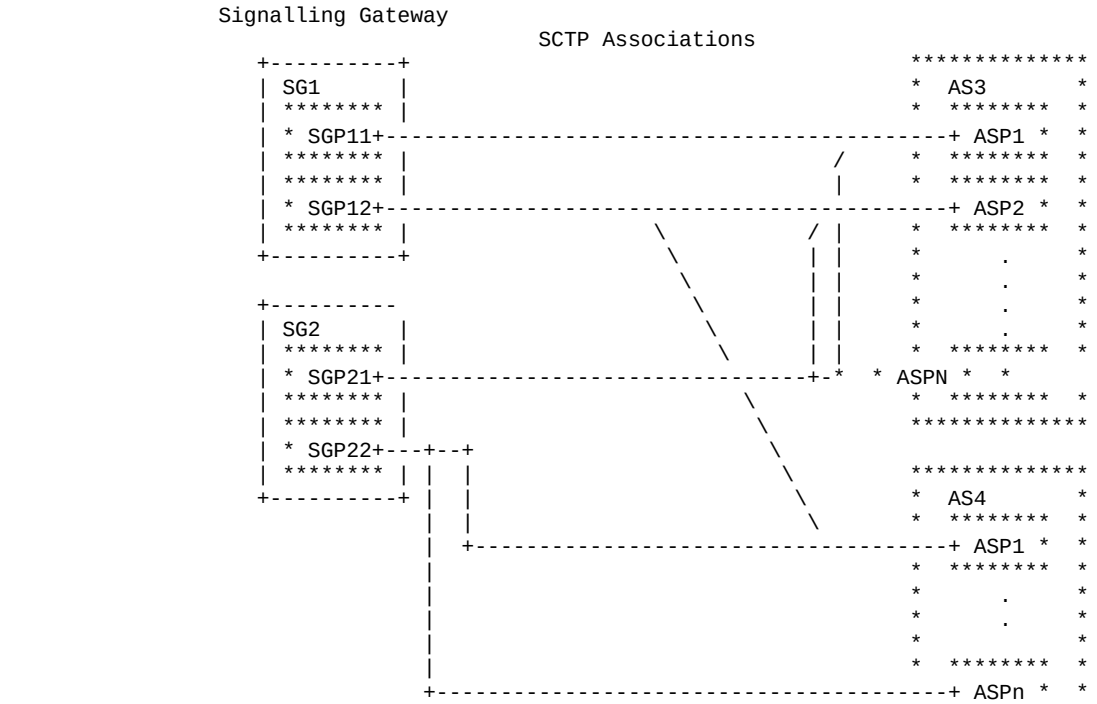


Figure 2: Signalling Gateway Architecture

The pair of SGs can either operate as replicated endpoints or as replicated relay points from the SS7 network point of view.

Replicated endpoints: the coupling between the SGs and the ASPs when the SGs act as replicated endpoints is an implementation issue.

Replicated relay points: in normal circumstances, the path from SEP to ASP will always go via the same SGP when in-sequence-delivery is requested. However, linkset failures may cause MTP to re-route to the other SG.

A.3 Signaling Gateway Message Distribution Recommendations

A.3.1 Connectionless Transport

By means of configuration, the SG knows the local SCCP-user is actually represented by an AS, and serviced by a set of ASPs working

in n+k redundancy mode. An ASP is selected and a CLDT message is sent on the appropriate SCTP association/stream.

The selection criterion can be based on a round robin mechanism, or any other method that guarantees a balanced load sharing over the active ASPs. However, when TCAP messages are transported, load sharing is only possible for the first message in a TCAP dialogue (TC_Begin, TC_Query, TC_Unidirectional). All other TCAP messages in the same dialogue are sent to the same ASP that was selected for the first message, unless the ASPs are able to share state and maintain in sequence delivery. To this end, the SGP needs to know the TID allocation policy of the ASPs in a single AS:

- State sharing
- Fixed range of TIDs per ASP in the AS

This information may be preconfigured in the SG, or may be dynamically exchanged via the ASP_Active message.

An example for an INAP/TCAP message exchange between SEP and ASP is given below.

Address information in CLDT message (e.g. TC_Query) from SGP to ASP, with association ID = SG-ASP, Stream ID based on sequence control and possibly other parameters, e.g. OPC:

- Routing Context: based on SS7 Network ID and AS membership, so that the message can be transported to the correct ASP.
- Source address: valid combination of SSN, PC and GT, as needed for back routing to the SEP.
- Destination address: at least SSN, to select the SCCP/SUA-user at the ASP.

Address information in CLDT message (e.g. TC_Response) from ASP to SG, with association ID = ASP-SG, stream ID selected by implementation dependent means with regards to in-sequence-delivery:

- Routing Context: as received in previous message.
- Source address: unique address provided so that when used as the SCCP called party address in the SEP, it must yield the same AS, the SSN might be sufficient.
- Destination address: copied from source address in received CLDT message.

Further messages from the SEP belonging to the same TCAP transaction will now reach the same ASP.

A.3.2 Connection-Oriented Transport

Further messages for this connection are routed on DPC in the SS7 connection section (MTP routing label), and on IP address in the IP connection section (SCTP header). No other routing information is

present in the SCCP or SUA messages themselves. Resources are kept within the SG to forward messages from one section to another and to populate the MTP routing label or SCTP header, based on the destination local reference of these messages (Connect Confirm, Data Transfer, etc.)

This means that in the SG, two local references are allocated, one 3-byte value used for the SS7 section and one 4-byte value for the IP section. Also a resource containing the connection data for both sections is allocated, and either of the two local references can be used to retrieve this data e.g. for an incoming DT1 or CODT, for example.

Copyright Statement