INTERNET-DRAFT
Engineering Task Force

J. Loughney Internet
Nokia
G. Sidebottom, Guy Mousseau
Nortel Networks
S. Lorusso
Unisphere Solutions

Issued: 8 March 2000
Expires: 8 September 2000

SS7 SCCP-User Adaptation Layer (SUA)
<draft-loughney-sigtran-sua-00.txt>

Status of This Memo

Abstract

This Internet Draft defines a protocol for the transport of any SS7 SCCP-User signaling (e.g., TCAP, RANAP, etc.) over IP using the Simple Control Transport Protocol. Protocol elements are added to enable a seamless operation of the SCCP-User peers in the SS7 and IP domains. This protocol could be used between a Signaling Gateway (SG) and an IP-based signaling node (or an IP-resident Database). It is assumed that the SG receives SS7 signaling over a standard SS7 interface using the SS7 Signaling Connection Control Part (SCCP) to provide transport from the SS7 network to the SG.

1. Introduction

1.1 Scope

There is on-going integration of SCN networks and IP networks. IP provides an effective way to transport user data, as well as for operators to expand their networks. This document details the delivery of SCCP-user messages (MAP & CAP over TCAP, RANAP, etc.) over IP, from an SS7 Signaling Gateway (SG) to an IP-based signaling node (such as an IP-resident Database) as described in the Framework Architecture for Signaling Transport [1]. The delivery mechanism SHOULD meet the following criteria:

* Support for transfer of SS7 SCCP-User Part messages (e.g., 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 an SG and one or more IP-based signaling nodes).
* Support for distributed IP-based signaling nodes.
* Support for the asynchronous reporting of status changes to management

In other words, the SG will terminate SS7 MTP layers and SCCP layer and deliver TCAP, RANAP and/or any other SCCP-User protocol messages over SCTP associations to SCCP-User peers in distributed IP-Based signaling nodes. Depending upon the SCCP-users supported, the SUA will need to support SCCP connectionless service, SCCP connect-orient service or both services.

1.2 Terminology

Application Server (AS) - A logical entity serving a specific Routing Key. An example of an Application Server is a virtual switch element handling all call processing for a unique range of PSTN trunks, identified by an SS7 DPC/OPC/SSN. 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 standby process of an Application Server (e.g., part of a distributed virtual switch 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.

Association - An association refers to an SCTP association. The association provides the transport for the delivery of MTP3-User

protocol data units and M3UA adaptation layer peer messages.

Routing Key - At the SG, the Routing Key describes a set of SS7 parameter/parameter-ranges that uniquely defines the range of signaling traffic configured to be handled by a particular Application Server. An example would be where a Routing Key consists of a particular DPC and SSN to which all traffic would be directed to a articular Application Server. Routing Keys are mutually exclusive in the sense that a received SS7 signaling message cannot be directed to more than one Routing Key. A Routing Key cannot extend across more than a single SS7

DPC, in order to more easily support SS7 Management procedures. It is not necessary for the parameter ranges within a particular Routing Key to be contiguous.

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 SG and the ASP, identifying the relevant Application Server. From the perspective of an ASP, the Routing Context uniquely identifies the range of traffic associated with a particular Application Server, which the ASP is configured to receive from the SG. There is a 1:1 relationship between a Routing Context value and a Routing Key at an SG. Therefore the Routing Context can be viewed as an index into an SG Table containing the SG Routing Keys.

Fail-over - The capability to re-route signaling 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-back may apply upon the return to service of a previously unavailable Application Server Process.

Signaling Point Management Cluster (SPMC) - A complete set of Application Servers represented to the SS7 network under the same SS7 Point Code. SPMCs are used to sum the availability/congestion/User_Part status of an SS7 destination point code that is distributed in the IP domain, for the purpose of supporting MTP Level 3 management procedures at an SG.

Network Appearance - The Network Appearance identifies an SS7 network context for the purposes of logically separating the signaling traffic between the SG and the Application Server Processes over a common SCTP Association. An example is where an SG is logically partitioned to appear as an element in four separate national SS7 networks. A Network Appearance implicitly defines the SS7 Point Code(s), Network Indicator and MTP3 protocol type/variant/version used within a specific SS7 network partition. An physical SS7 route-set or link-set at an SG can appear in only one network appearance. The Network Appearance is not globally significant and requires coordination only between the SG and the ASP.

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

Layer Management - Layer Management is a nodal function in an SG or ASP that handles the inputs and outputs between the M3UA layer and a local management entity.

Host - The computing platform that the 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 which 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.

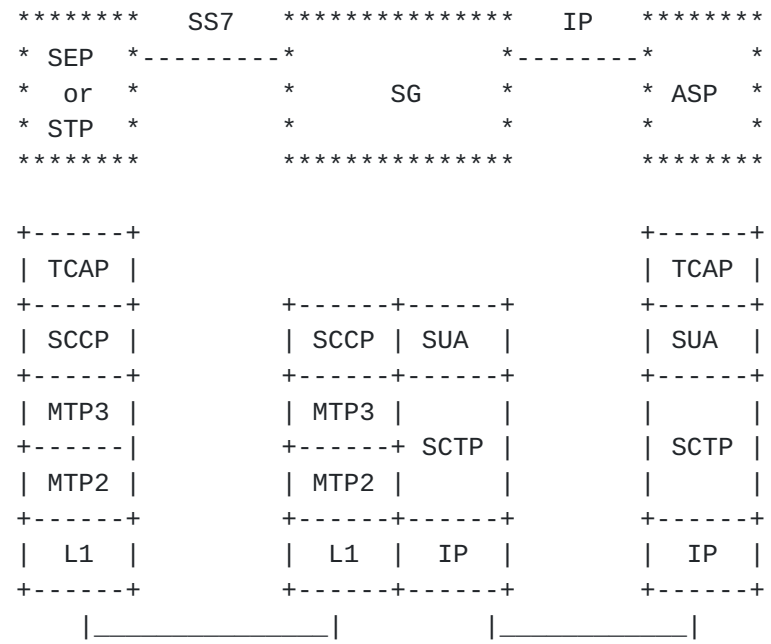
1.3 Signaling Transport Architecture

The framework architecture that has been defined for SCN signaling transport over IP [1] uses multiple components, including an IP transport protocol, a signaling common transport protocol and an adaptation module to support the services expected by a particular SCN signaling protocol from its underlying protocol layer.

In general terms, the architecture can be modeled as a client-server architecture, where SG acts as the server and the ASP acts as the client.

1.3.1 Protocol Architecture for TCAP Transport

In this architecture, the SCCP and SUA layers interface in the SG. There needs to be interworking between these layers to provide for the seamless transfer of the user messages as well as the management messages. The SUA handles the SS7 address to IP address mapping.

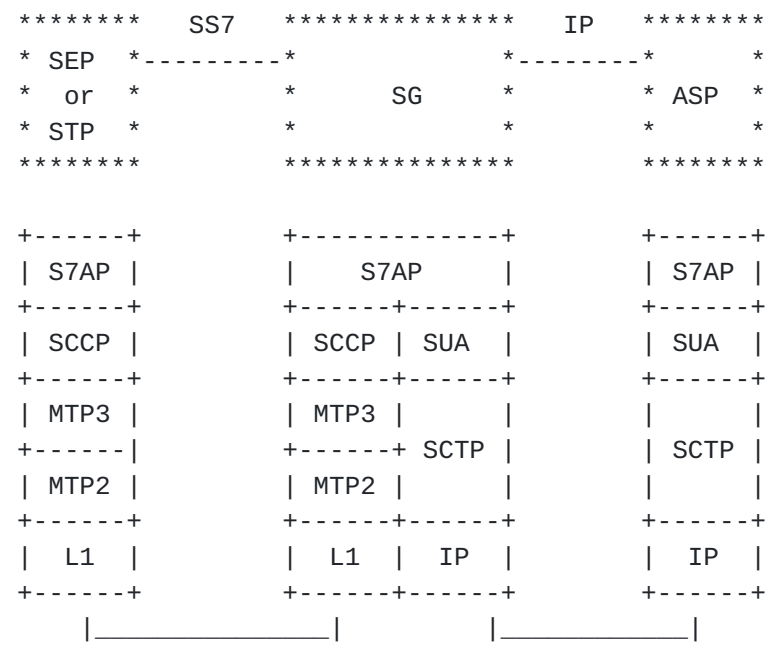


TCAP - Transaction Capability Application Protocol
STP - SS7 Signaling Transfer Point

1.3.2 Protocol Architecture for RANAP Transport

In this architecture, the SS7 application protocol is invoked at the SG. For messages destined for an ASP, the SUA handles address translation, for example by way of Global Title Translation or via mapping table,

resolving the destination specified by SS7 Application to a SCTP association / IP address.



S7AP - SS7 Application Protocol (e.g. - RANAP/RNSAP)
STP - SS7 Signaling Transfer Point

This architecture may simplify, in some cases, to carrying an SS7 application protocol between two IP based endpoints. In this scenario, full SG functionality may not be needed. This architecture is considered in Annex A.

1.3.3 IP-Based Signaling Network Architecture

The Signaling Gateway (SG) is the gateway node between the SS7 network and the IP network. The SG will transport SCCP-user signaling traffic from the SS7 network to the IP-based signaling nodes (for example IP-resident Databases). The SUA protocol does not specify the performance and reliability requirements needed for the transport of user signaling, but relies on SCTP and the layers below to provide it. 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.

It is recommended that when realizing this protocol, the network architecture allows for multiple hosts, to be attached to the SG(s). Multiple associations can be used between the SGs and hosts to provide failover scenarios. Also, it is advisable for several ASPs to be located within the hosts, again for failover use.

Figure 1 shows an example network architecture which can support robust operation and failover support.

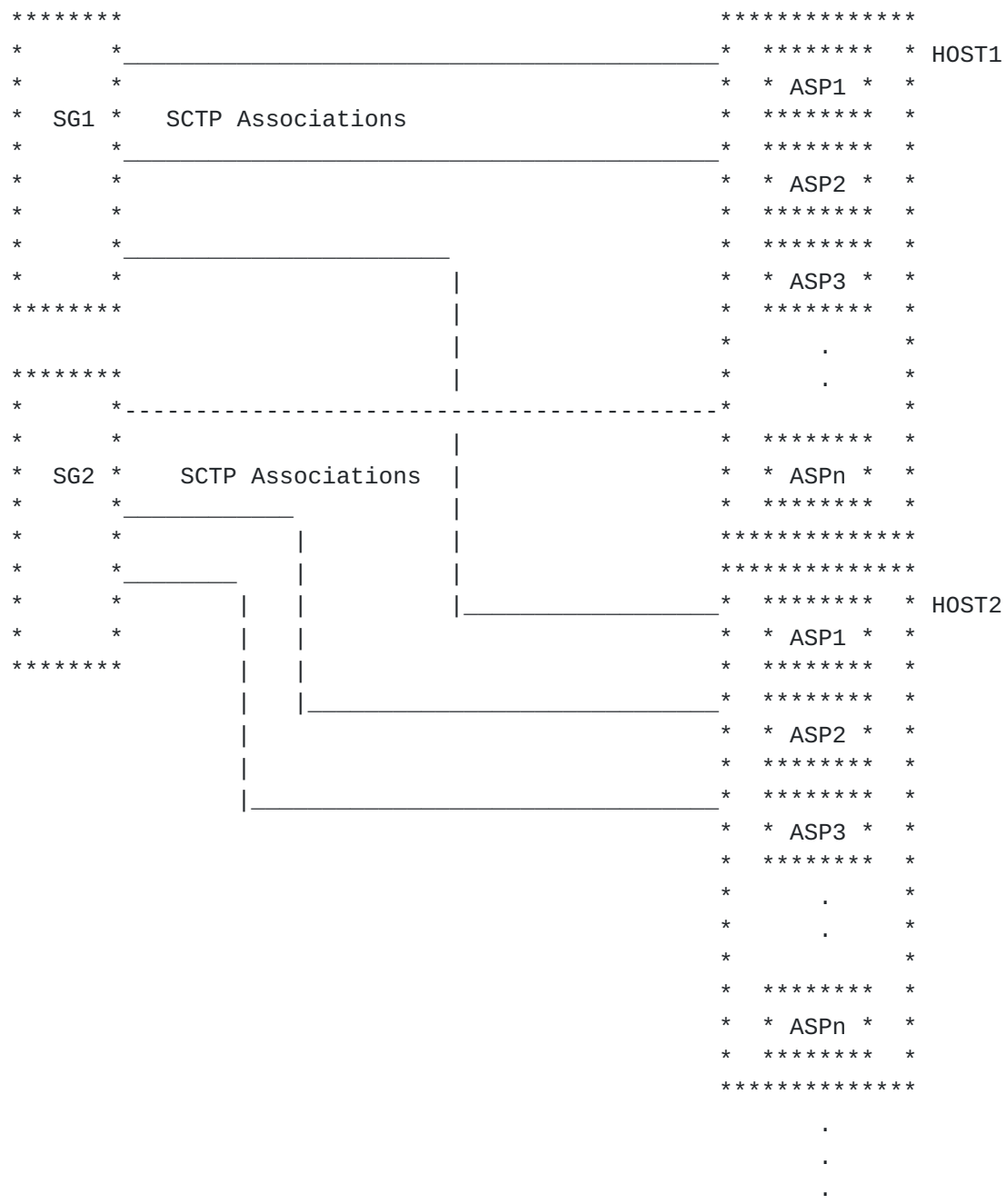


Figure 1 - Physical Model

1.3.4 ASP Fail-over Model and Terminology

The network address translation and mapping function of the SUA supports ASP fail-over functions in order to support a high availability of

transaction processing capability. The SUA at the SG assign a unique Application Server to all SCCP-user messages incoming from the SS7 network based on some information in the SCCP-user message. The SUA at the SG may use a combination of the following information to make the AS/ASP assignment:

- Destination Point Code (DPC)
- Originating Point Code (OPC)
- Sub-System Number (SSN)
- Global Title (GT)

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 while any others are inactive but available in the event of failure or unavailability of the active ASP(s).

The fail-over model supports an "n+k" redundancy model, where "n" ASPs is the minimum number of redundant ASPs required to handle traffic and "k" ASPs are available to take over for a failed or unavailable ASP. Note that "1+1" active/standby redundancy is a subset of this model. A simplex "1+0" model is also supported as a subset, with no ASP redundancy.

To avoid a single point of failure, it is recommended that a minimum of two ASPs be resident in the list, resident in separate physical hosts and therefore available over different SCTP Associations.

1.4 Services Provided by the SUA Layer

1.4.1 Support for the transport of SCCP-User Messages

The SUA needs to support the transfer of SCCP-user messages. The SUA layer at the SG needs to seamlessly transport the SCCP-user messages.

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 signaling 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 may provide management of the underlying SCTP layer to ensure that SG-ASP transport is available according to the degree specified by the SCCP-user application.

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

The SUA layer needs to support the following SCCP network management functions:

Coord Request
Coord Indication
Coord Response
Coord Confirm
State Request
State Indication
Pcstate Indication

1.4.5 Support for the management between the SG and ASP.

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

1.5 Internal Functions Provided in the SUA Layer

1.5.1 Address Translation and Mapping at the SG

SCCP users may present the following options to address their peer endpoints:

Global Title
DPC + SSN
OPC + SSN

If Global Titles are used, the rules detailed in Annex B of ITU Q.713 [2] should be consulted.

1.5.2 SCTP Stream Mapping

The SUA supports SCTP streams. The SG 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 MUST use stream 0 for SUA management messages. Stream 0 MUST support sequenced delivery, in order to preserve the order of management message delivery.

1.5.3 Congestion Control

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.

Connect Request
Connect Indication
Connect Responding
Connect Confirm
Data Request
Data Indication
Expedited Data Request
Expedited Data Indication
Disconnect Request
Disconnect Indication
Reset Request
Reset Indication
Reset Response
Reset Confirm

1.6.2 Definition of the lower boundary

The upper layer primitives provided by the SCTP are provided in [7].

1.6.3 SUA Peer Messages

data transfer
data acknowledge
connection request
connection acknowledge
release request
release complete
reset confirm
reset request
ASP Up
ASP Down
ASP Active
ASP Inactive
ASP Takeover
Notify
No Active ASP
Error
Audit
Stream Configuration
Stream Configuration Acknowledge
Destination Unavailable
Destination Available
Destination State Audit
SS7 Network Congestion State
Destination User Part Unavailable
Vendor-Specific Message

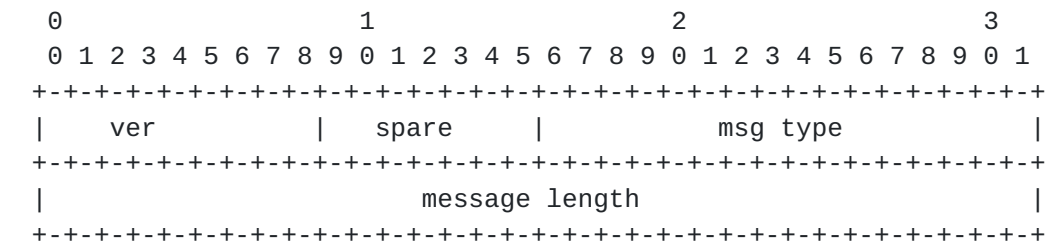
2 Protocol Elements

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.

2.1 Common Message Header

The protocol messages for SCCP-User Adaptation require a message

structure which contains a version, message type, message length, and message contents. This message header is common among all signaling protocol adaptation layers:



2.1.1 SUA Protocol Version

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

01 SUA version 1.0

2.1.2 Message Types

Data Transfer Messages

Data Transfer (DATR)	0x0501
Data Acknowledge (DAAC)	0x0502

Connection Messages

connection request (CORE)	0x0601
connection acknowledge (COAK)	0x0602
release request (RELRE)	0x0603
release complete (RELCO)	0x0604
reset confirm (RESCO)	0x0605
reset request (RESRE)	0x0606

Application Server Process Maintenance (ASPM) Messages

ASP Up (ASPUP)	0x0301
ASP Down (ASPDN)	0x0302
ASP Active (ASPAC)	0x0401
ASP Inactive (ASPIA)	0x0402
ASP Takeover (ASPTO)	0x0403
Notify (NTFY)	0x0404
No Active ASP (NAASP)	0x0405

SUA Management Messages

Error (ERR)	0x0001
Audit (AUD)	0x0002

Stream Configuration (SCO)	0x0003
Stream Configuration Acknowledge (SCA)	0x0004

SS7 Signaling Network Management (SSNM) Messages

Destination Unavailable (DUNA)	0x0201
Destination Available (DAVA)	0x0202
Destination State Audit (DAUD)	0x0203
SS7 Network Congestion State (SCON)	0x0204
Destination User Part Unavailable (DUPU)	0x0205

Other

Vendor-Specific Message (VEN) 0xFFFE

2.1.3 Message Length

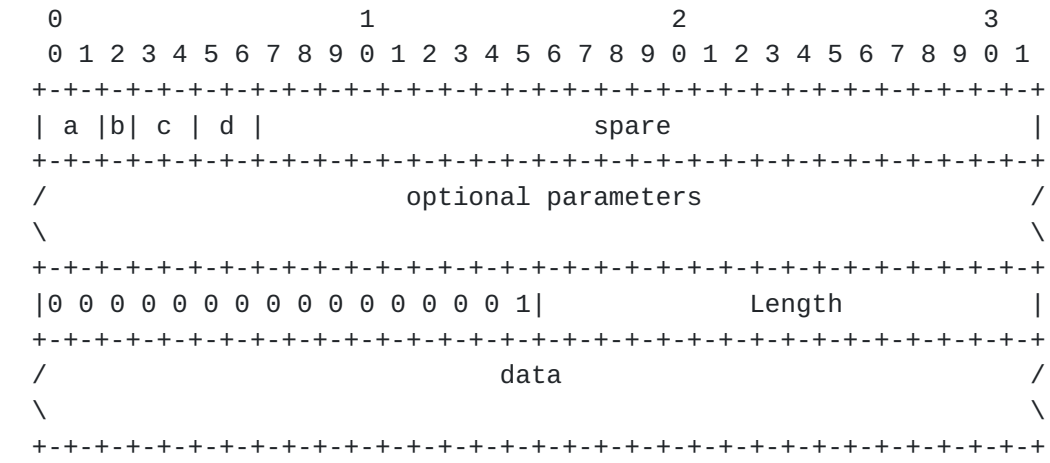
The Message Length defines the length of the message in octets, including the header.

2.2 SUA Transfer Messages

The following section describes the SUA 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.

2.2.1 Data Transfer

This message transfers data between one SUA to another.



Flags

A class
B priority
C ack
D segmentation

The class flag indicates which SCCP class this data transfer is supporting. The valid values for class are shown in the following table.

Value	Description
0x0	Class 0 (connectionless service)
0x1	Class 1 (connectionless service)
0x2	Class 2 (connection-oriented service)

0x3	Class 3 (connection-oriented service)

The priority parameter indicates if the data expects expedited services. The valid values are:

Value	Description
0x0	Normal priority
0x1	Expedited priority

The acknowledge flag indicates the receiving end should send an acknowledgement on receiving the data message. The valid values are:

Value	Description
0x0	No acknowledgement
0x1	Acknowledge on error
0x2	Acknowledgement required

The segmentation flag indicates if message segmentation is present. The valid values for segmentation are:

Value	Description
0x0	No segmentation
0x1	First piece of segmented data
0x2	middle piece of segmented data
0x3	final piece of segmented data

Optional parameters include:

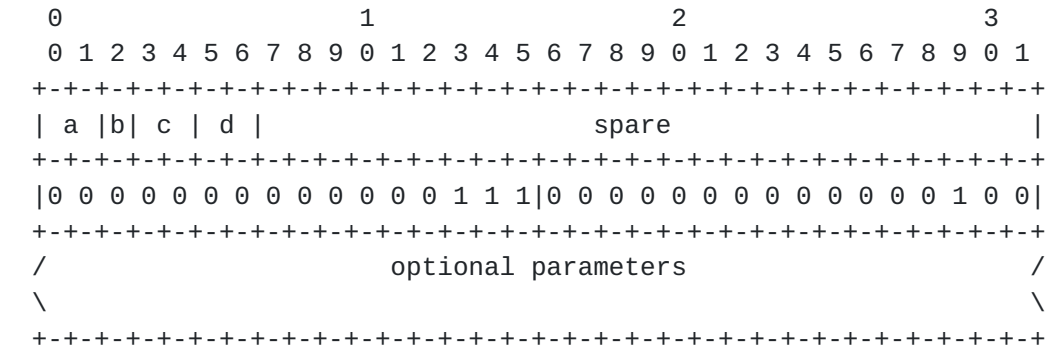
Sequence number
source reference number
destination reference number
sending address
destination address

Section 2.8 defines the format (in TLV format) for the optional paramters.

Implementation note:

This message covers the following SCCP messages: unitdata (UDT), extended unitdata (XUDT), data form 1 (DT1), data form 2 (DT2), expedited data (ED), long unitdata (LUDT).

2.2.2 Data Acknowledge



Flags

A	class
B	priority
C	ack
D	segmentation

The class flag indicates which SCCP class this data transfer is supporting. The valid values for class are shown in the following table.

Value	Description
0x0	Class 0 (connectionless service)

0x1	Class 1 (connectionless service)
0x2	Class 2 (connection-oriented service)
0x3	Class 3 (connection-oriented service)

The priority parameter indicates if the data expects expedited services. The valid values are:

Value	Description
0x0	Normal priority
0x1	Expedited priority

The acknowledge flag is set to 0

The segment parameter is set to 0.

Reason code MUST be included. See section 2.8 for additional details.

Optional parameters include:

- data
- cause
- sequence number
- destination reference number
- sending address
- destination address

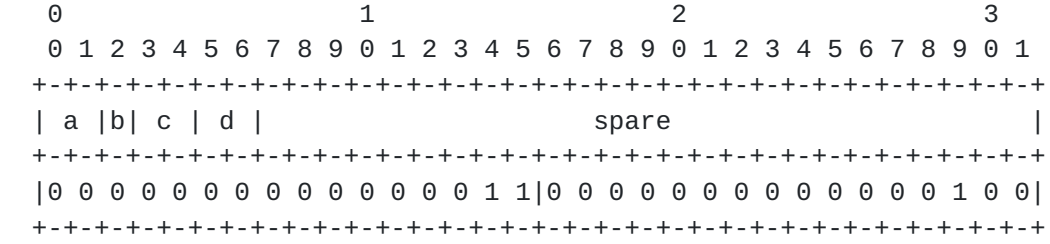
Implementation note:

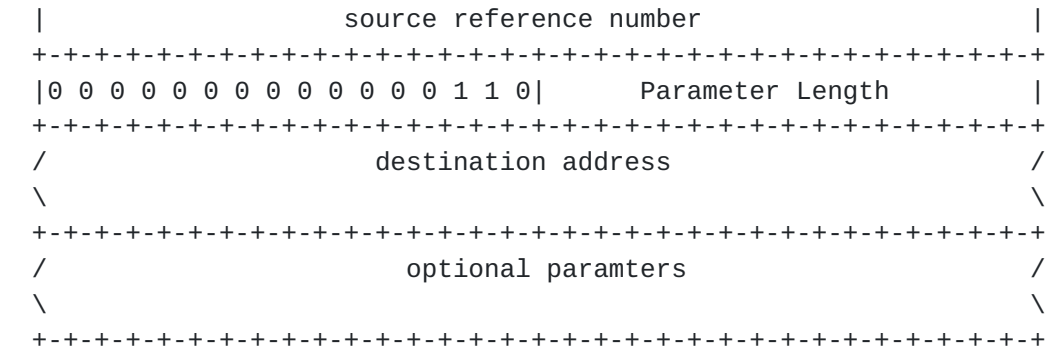
This message covers the following SCCP messages: protocol data unit error (ERR), long unitdata service (LUDTS), unitdata service (UDTS), extended unitdata service (XUDTS), data acknowledgement (AK), expedited data acknowledgement (EA).

2.3 Connection Messages

The connection messages are used in the connection-oriented services provided by the SUA, indicated by protocol class 2 or 3. The release messages are used only for SCCP-users requesting protocol class 3.

2.3.1 Connection Request




source reference number
0 0 0 0 0 0 0 0 0 0 0 0 1 1 0
Parameter Length
destination address
optional paramters

Flags

A class
B priority
C ack
D segmentation

The class flag indicates which SCCP class this data transfer is supporting. The valid values for class are shown in the following table.

Value	Description
0x2	Class 2 (connection-oriented service)
0x3	Class 3 (connection-oriented service)

The priority flag indicates if the data expects expedited services. The valid values are:

Value	Description
0x0	Normal priority
0x1	Expedited priority

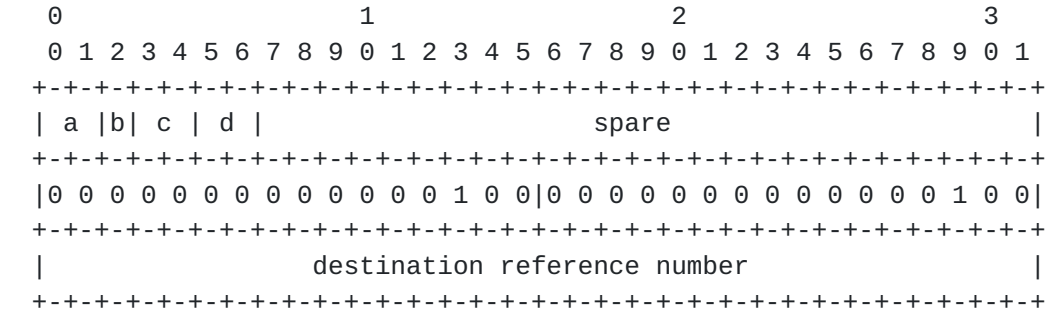
The acknowledge flag is not used, it MUST be set to 0.

The segmentation flag is not used, it MUST be set to 0.

Optional parameters include:

Data
Sending Address

2.3.2 Connection Acknowledge



Flags

A class
B priority
C ack
D segmentation

The class flag indicates which SCCP class this data transfer is supporting. The valid values for class are shown in the following table.

Value	Description
0x2	Class 2 (connection-oriented service)
0x3	Class 3 (connection-oriented service)

The priority flag indicates if the data expects expedited services. The valid values are:

Value	Description
0x0	Normal priority
0x1	Expedited priority

The acknowledge flag is not used, it MUST be set to 0.

The segmentation flag is not used, it MUST be set to 0.

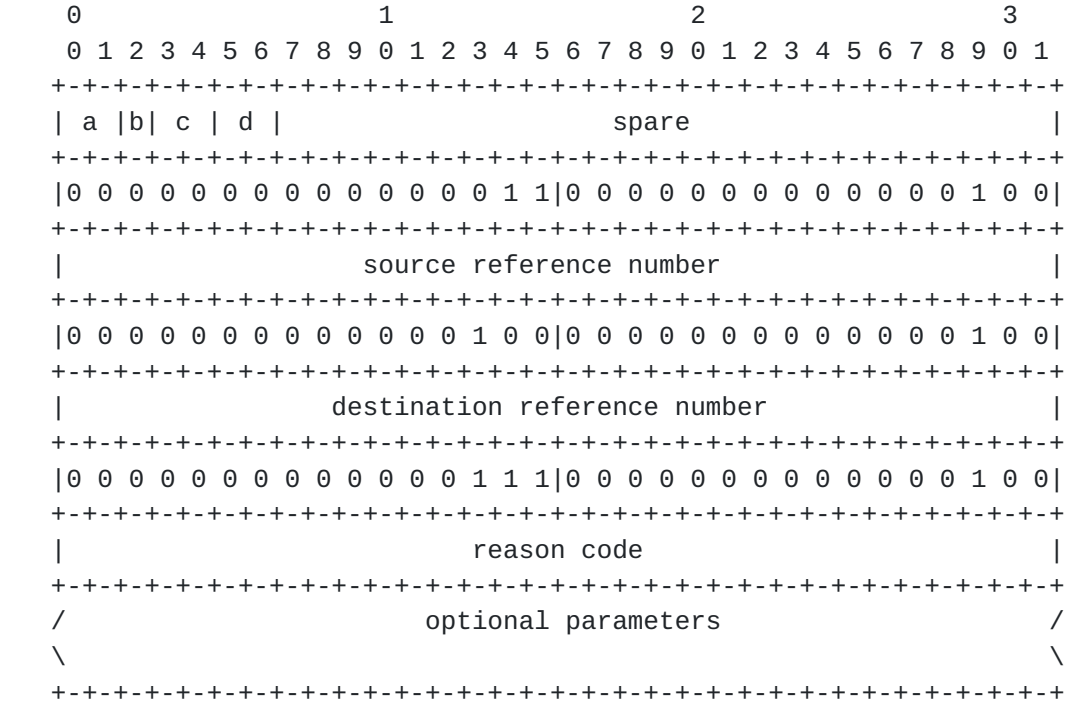
Optional parameters include:

- Data
- cause
- Source reference number
- destination reference number
- destination address

Implementation note:

This message covers the following SCCP messages: connection confirm (CC), connection refused (CREF).

2.3.3 Release Request



Flags

A	class
B	priority

C	ack
D	segmentation

The class flag indicates which SCCP class this data transfer is supporting. The valid values for class are shown in the following table.

Value	Description
0x2	Class 2 (connection-oriented service)
0x3	Class 3 (connection-oriented service)

The priority parameter indicates if the data expects expedited services. The valid values are:

Value	Description
0x0	Normal priority
0x1	Expedited priority

The acknowledge flag is not used, it MUST be set to 0.

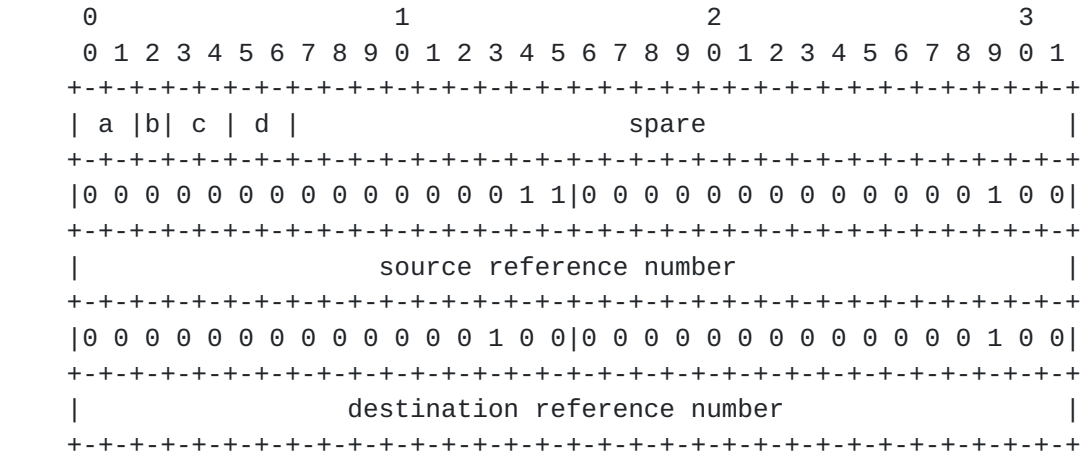
The segmentation flag is not used, it MUST be set to 0.

Optional parameters include:

- data
- result

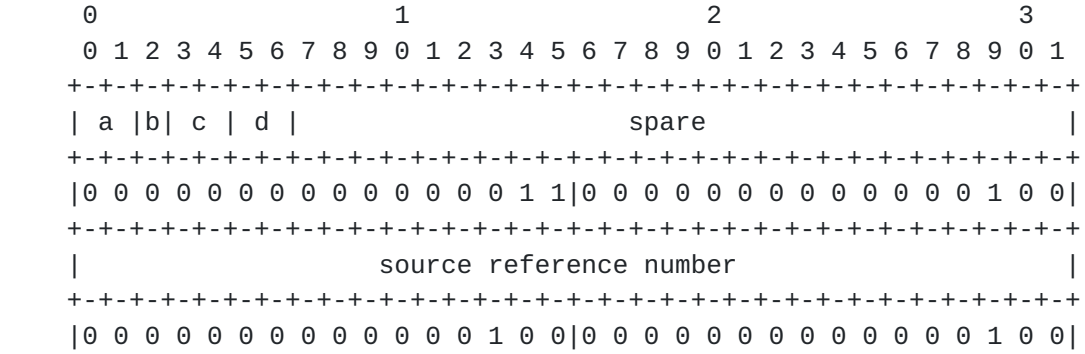
Section 2.8 defines the format (in TLV format) for the optional paramters.

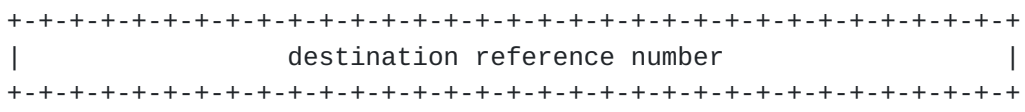
2.3.4 Release Complete



All flags MUST be set to 0.

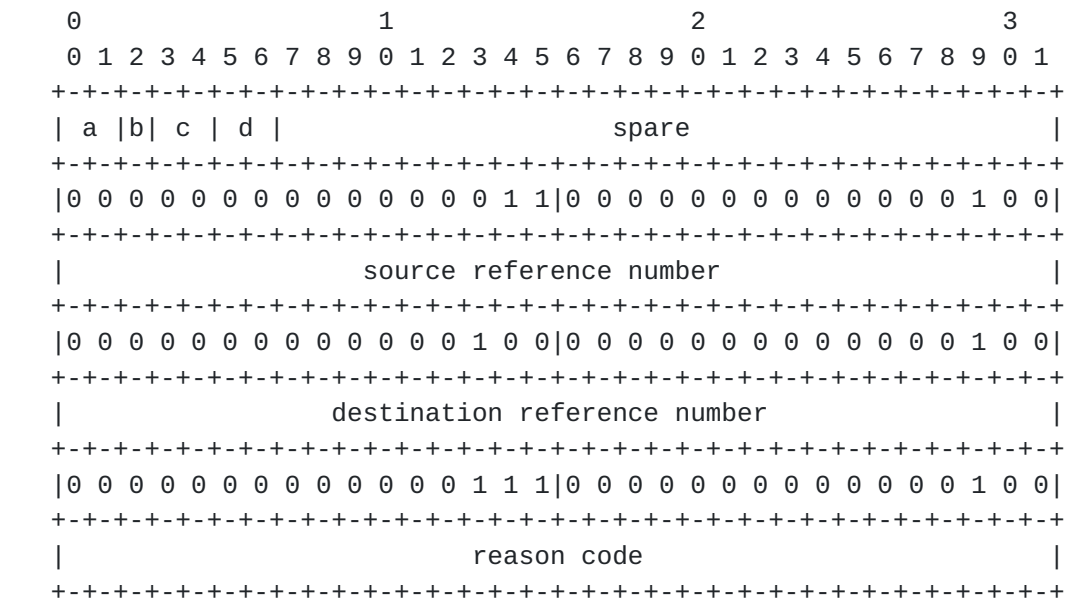
2.3.5 Reset Confirm





All flags MUST be set to 0.

2.3.6 Reset Request



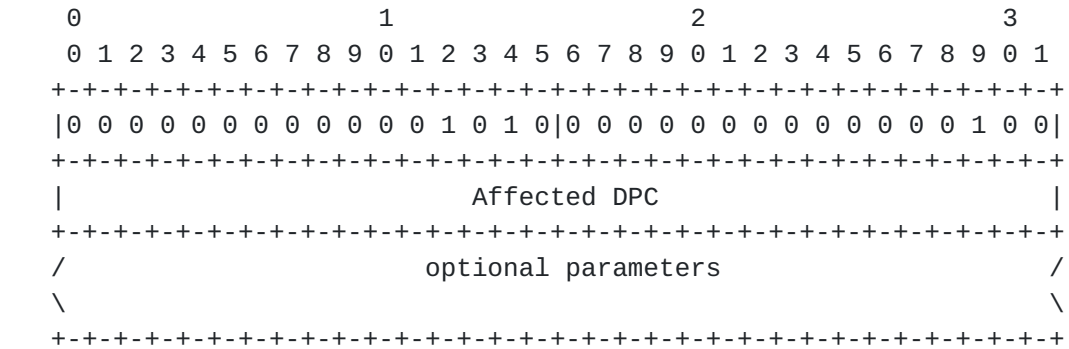
All flags MUST be set to 0.

2.4 SS7 Signaling Network Management Messages

2.4.1 Destination Unavailable

The DUNA message is sent from the SG to all concerned ASPs to indicate that the SG has determined that an SS7 destination is unreachable. The MTP3-User at the ASP is expected to stop traffic to the affected destination through the SG initiating the DUNA.

The format for DUNA Message parameters is as follows:



The DUNA message contains the following parameters:

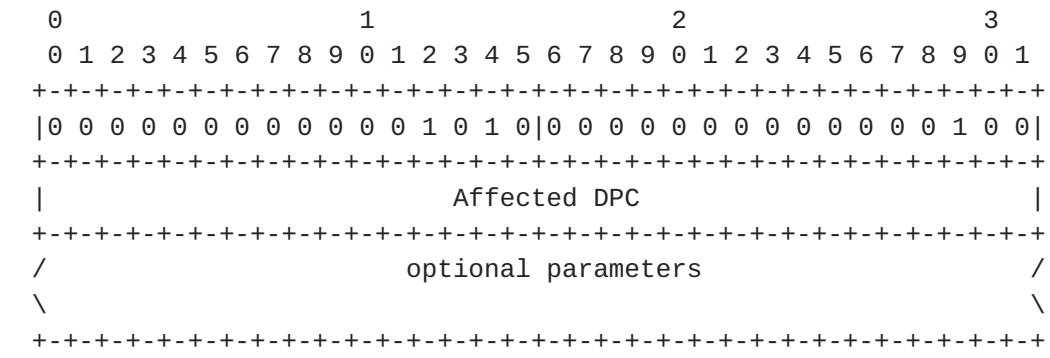
Affected Destination Point Code

Optional parameters include:

Protocol Identifier
Network Appearance
Info String

2.4.2 Destination Available

The DAVA message is sent from the SG to all concerned ASPs to indicate that the SG has determined that an SS7 destination is now reachable. The ASP MTP3-User protocol is expected to resume traffic to the affected destination through the SG initiating the DUNA.



The DUNA message contains the following parameters:

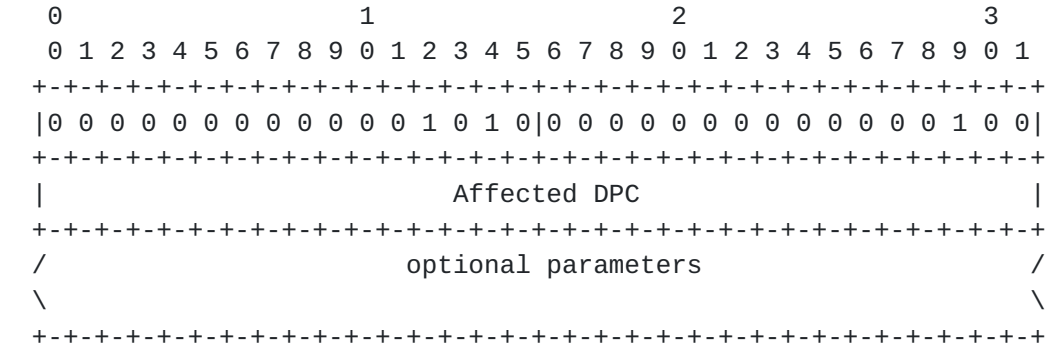
Affected Destination Point Code

Optional parameters include:

Protocol Identifier
Network Appearance
Info String

2.4.3 Destination State Audit

The DAUD message can be sent from the ASP to the SG to query the availability state of the SS7 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.



The DUNA message contains the following parameters:

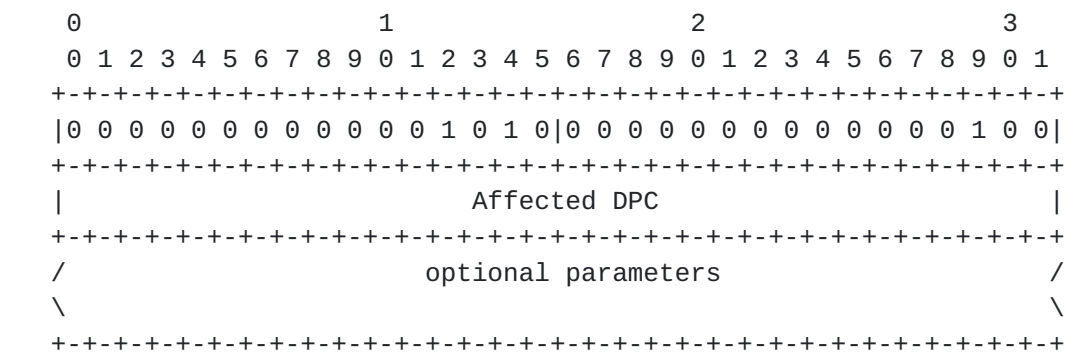
Affected Destination Point Code

Optional parameters include:

Protocol Identifier
Network Appearance
Info String

2.4.4 SS7 Network Congestion

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



The DUNA message contains the following parameters:

Affected Destination Point Code

Optional parameters include:

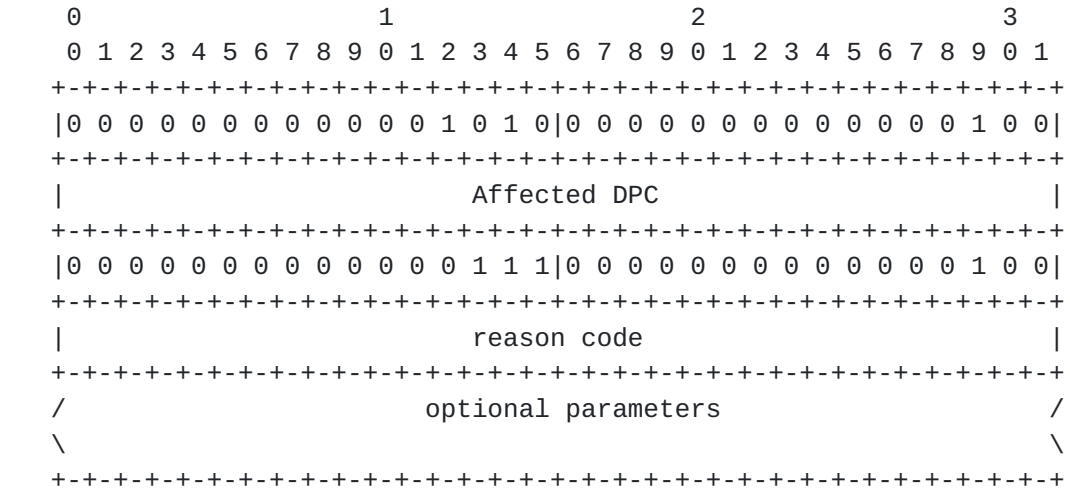
Protocol Identifier
Network Appearance
Info String
Congestion Level

Implementation note:

This message covers the following SCCP message: subsystem congested (SSC).

2.4.5 Destination User Part Unavailable

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



The DUPU message contains the following parameters:

Affected Destination Point Code
Reason

Optional parameters include:

Protocol Identifier
Network Appearance
Info String

2.5 Application Server Process Maintenance Messages

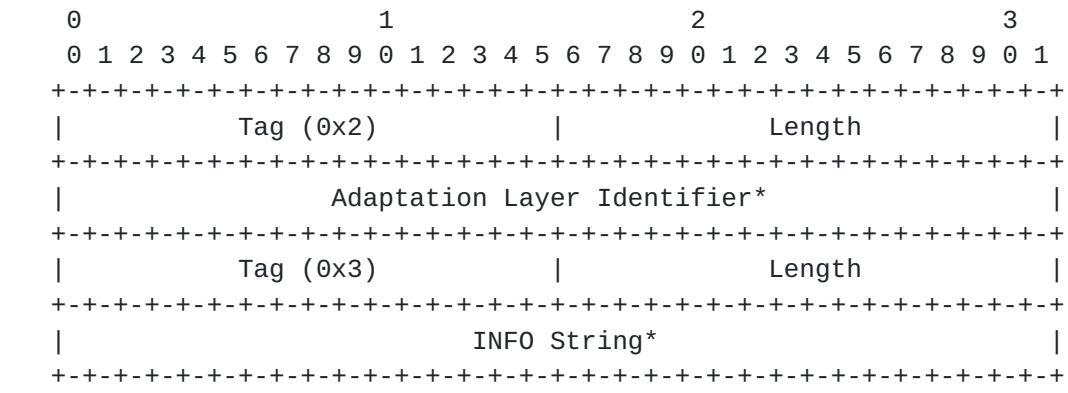
2.5.1 ASP Up (ASPUP)

The ASP UP (ASPUP) message is used to indicate to a remote M3UA peer that the Adaptation layer is ready to receive traffic or maintenance messages.

The ASPUP message contains the following parameters:

Adaptation Layer Identifier (optional)
INFO String (optional)

The format for ASPUP Message parameters is as follows:



The optional Adaptation Layer Identifier (ALI) is a string that identifies the adaptation layer. This string MUST be set to "SUA" which results in a length of 4. The ALI would normally only be used in the initial ASP Up message across a new SCTP association to ensure both peers are assuming the same adaptation layer protocol.

Note: Strings are padded to 32-bit boundaries. The length field indicates the end of the string.

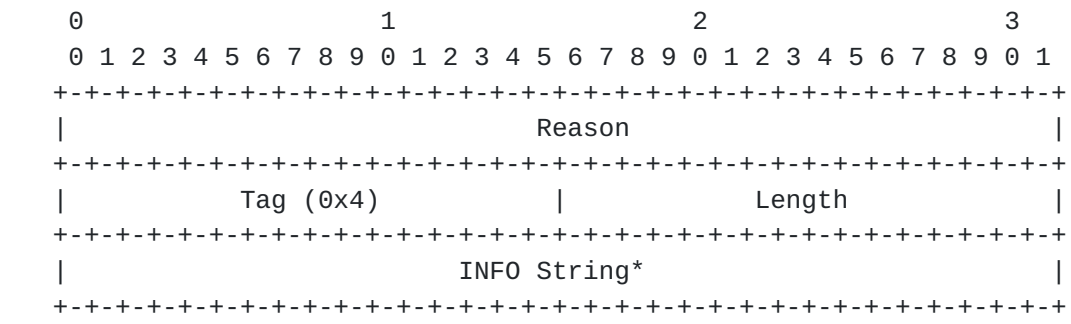
2.5.2 ASP Down (ASPDN)

The ASP Down (ASPDN) message is used to indicate to a remote M3UA peer that the adaptation layer is not ready to receive traffic or maintenance messages.

The ASPDN message contains the following parameters:

Reason
INFO String (Optional)

The format for the ASPDN message parameters is as follows:


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
Reason
Tag (0x4)
Length
INFO String*

The format and description of the optional Info String parameter is the same as for the DUNA message (See Section 2.3.2.1.)

The Reason parameter indicates the reason that the remote SUA adaptation layer is unavailable. The valid values for Reason are shown in the following table.

Value	Description
0x1	Processor Outage
0x2	Management Inhibit

Implementation note:

This message covers the following SCCP message: subsystem-prohibited (SSP).

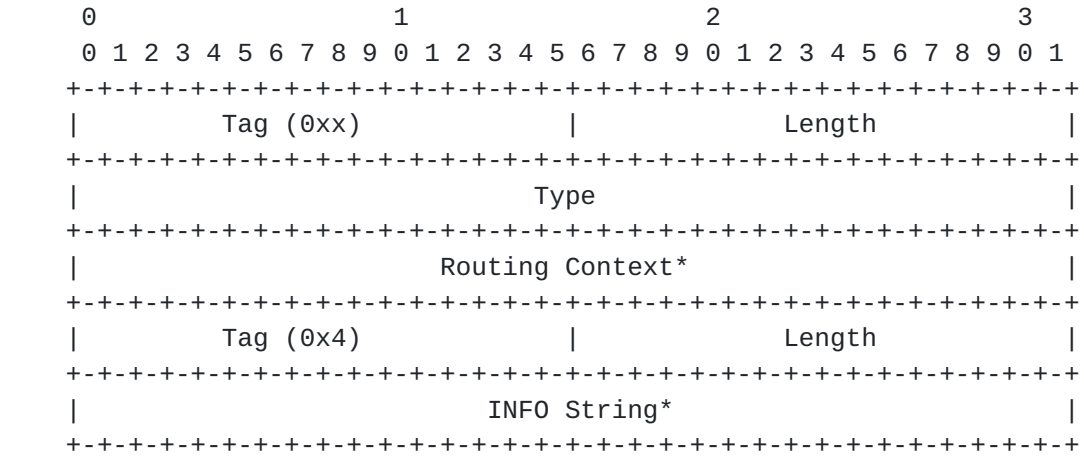
2.5.3 ASP Active (ASPAC)

The ASPAC message is sent by an ASP to indicate to an SG that it is Active and ready to be used.

The ASPAC message contains the following parameters:

Routing Context (Optional)
INFO String (Optional)

The format for the ASPAC message is as follows:



The Type parameter identifies the ASPAC as an Over-ride or Load-share Active message. The valid values for Type are shown in the following table.

Value	Description
0x1	Over-ride

0x2 Load-share

Within a particular Routing Context, only one Type can be used. An SG that receives an ASPAC with an incorrect type for a particular Routing Context will respond with an Error Message.

The optional Routing Context parameter contains (a list of) integers indexing the Application Server traffic that the sending ASP is configured to receive. There is one-to-one relationship between an index entry and an AS Name. Because an AS can only appear in one

Network Appearance, the Network Appearance parameter is not required in the ASPAC message

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 signaling traffic that the ASP is currently configured to receive from the SG. For example, an ASP could be configured to support call processing for multiple ranges of PSTN trunks and therefore receive related signaling traffic, identified by separate SS7 DPC/OPC.

The format and description of the optional Info String parameter is the same as for the DUNA message.

Implementation note:

This message covers the following SCCP message: subsystem-allowed (SSA).

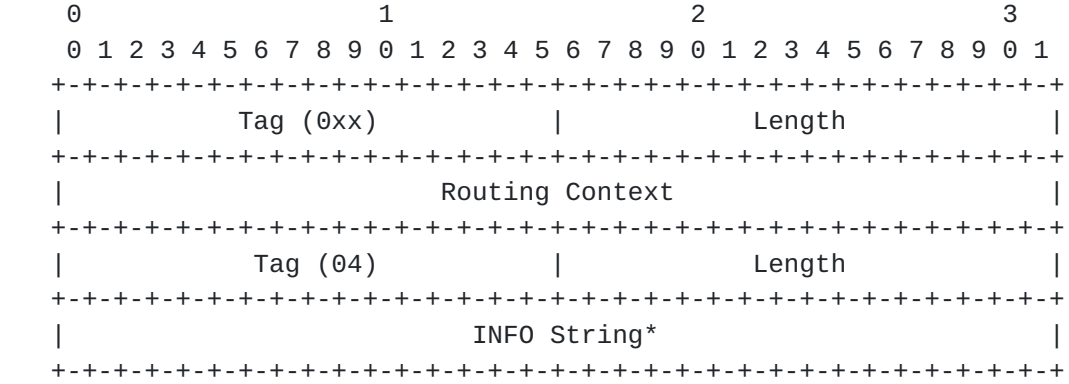
2.5.4 ASP Inactive (ASPIA)

The ASPIA message is sent by an ASP to indicate to an SG that it is no longer an active ASP to be used from within a list of ASPs. The SG will respond with an ASPIA message and either discard incoming messages or buffer for a timed period and then discard.

The contains the following parameters:

Routing Context (Optional)
INFO String (Optional)

The format for the ASPIA message parameters is as follows:



The format and description of the optional Routing Context and Info String parameters is the same as for the ASPAC message.

Implementation note:

This message covers the following SCCP message: subsystem-out-of-service-request (SOR).

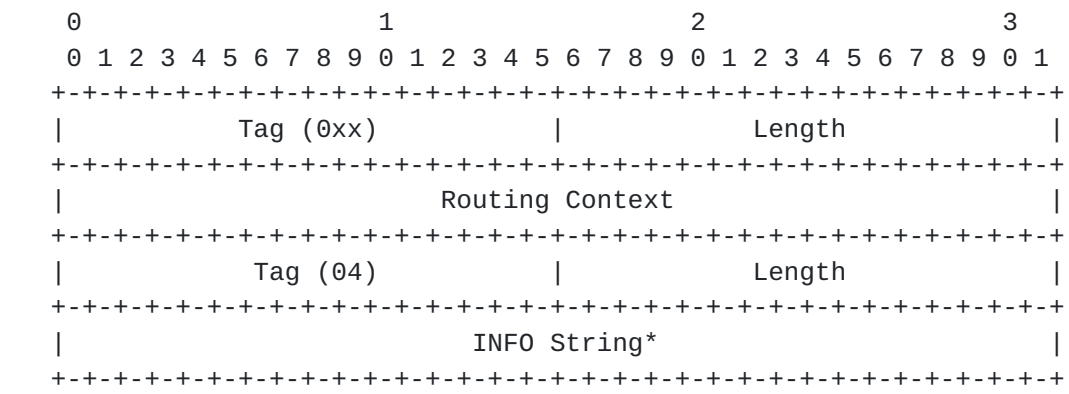
2.5.5 ASP Inactive Ack (ASPIAK)

The ASPIAK message is sent by the SG in response to an ASPIA to the sending ASP that it acknowledges the ASPIA.

The contains the following parameters:

Routing Context (Optional)
INFO String (Optional)

The format for the ASPIAK message parameters is as follows:



Implementation note:

This message covers the following SCCP message: subsystem-out-of-service-grant (SOG).

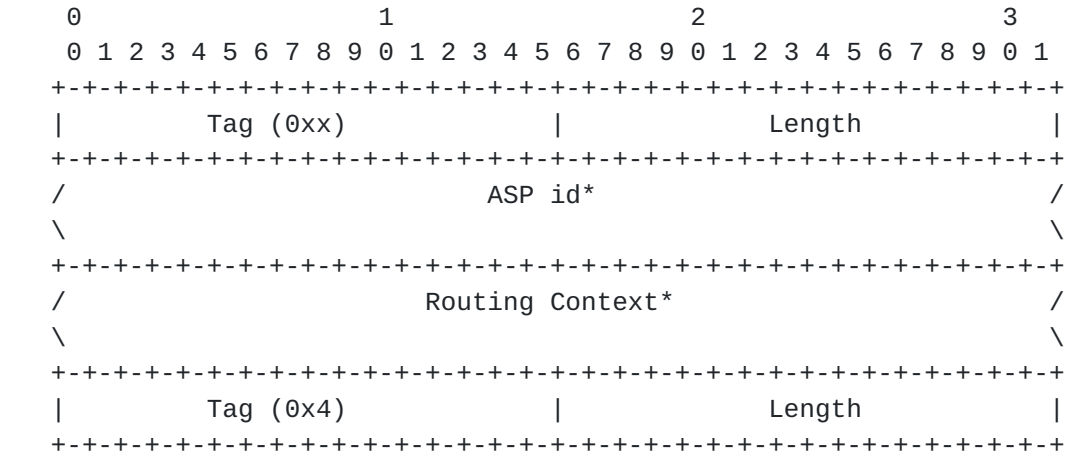
2.5.6 ASP Takeover (ASPTO)

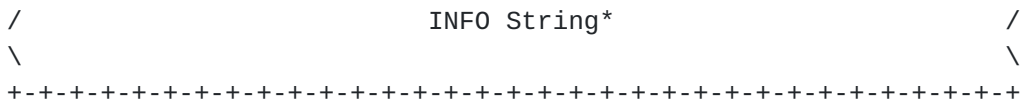
The ASPTO message is sent by an ASP to indicate to an SG that it will be replacing an active ASP, in a controlled manner.

The ASPTO message contains the following parameters:

Routing Context (Optional)
ASP id (Optional)
INFO String (Optional)

The format for the ASPAC message is as follows:





The optional ASP id parameter identifies an ASP, that will be taken over by the ASP that is sending this message. SG would keep sending traffic to both the ASPs for some time. Either because of a timer or an explicit ASPIA message from the taken over ASP, the SG would remove that ASP from the active ASPs list. During the time when both ASPs receive traffic,

all messages/traffic corresponding to new transactions/calls will be sent to the new ASP and traffic corresponding to the continued work would be sent to the old ASP.

The optional Routing Context parameter contains (a list of) integers indexing the Application Server traffic that the sending ASP is configured to receive. There is one-to-one relationship between an index entry and an AS Name. Because an AS can only appear in one Network Appearance, the Network Appearance parameter is not required in the ASPAC message

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 signaling traffic that the ASP is currently configured to receive from the SG. For example, an ASP could be configured to support call processing for multiple ranges of PSTN trunks and therefore receive related signaling traffic, identified by separate SS7 DPC/OPC_ranges.

The format and description of the optional Info String parameter is the same as for the DUNA message.

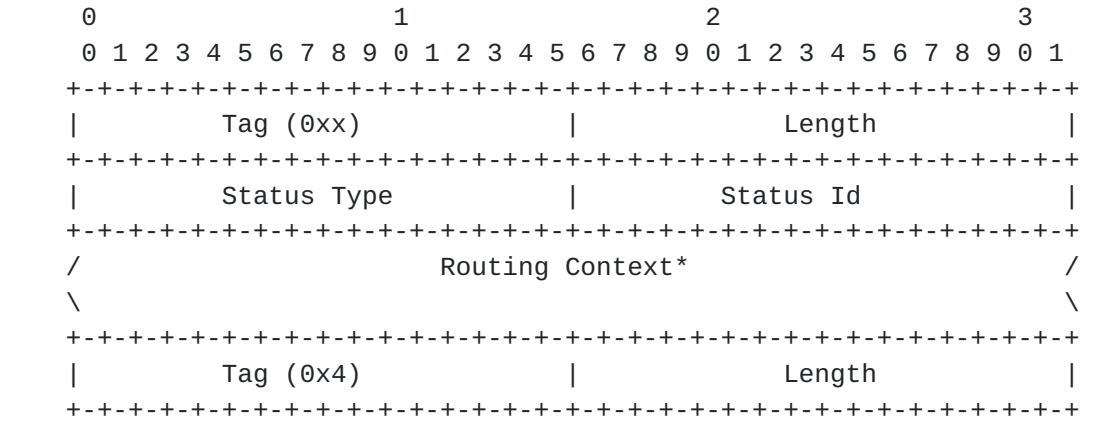
2.5.7 Notify (NTFY)

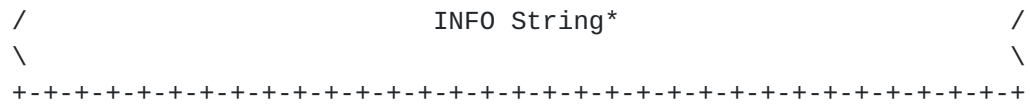
The NTFY message is sent by an SG to indicate any change of status in the AS or ASP to an ASP. SG sends this message to all concerned ASPs in an AS.

The NTFY message contains the following parameters:

- Status Type
- Status Id
- INFO String (Optional)

The format for the NTFY message parameters is as follows:





The Status Type parameter identifies the type of the status that is being notified. The valid values are shown in the following table.

Value	Description
0x1	AS_STATE_CHANGE

0x2	ASP_STATE_CHANGE

The Status Id parameter identifies the status that is being notified. The valid values are shown in the following table.

If the Status Type is AS_STATE_CHANGE

Value	Description
0x1	AS_DOWN
0x2	AS_UP
0x3	AS_PART_ACTIVE
0x4	AS_ACTIVE
0x5	AS_PENDING

If the Status Type is ASP_STATE_CHANGE

Value	Description
0x1	ASP_DOWN
0x2	ASP_UP
0x3	ASP_ACT_NEW
0x4	ASP_ACT_OLD
0x5	AS_ACTIVE

The format and description of the optional Routing Context and Info String parameters is the same as for the ASPAC message.

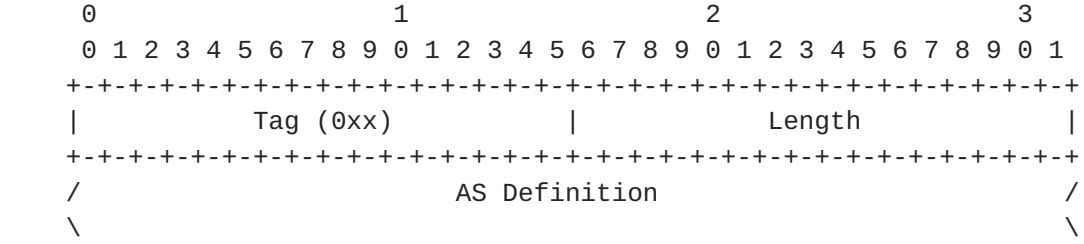
2.5.8 No Active ASP (NAASP)

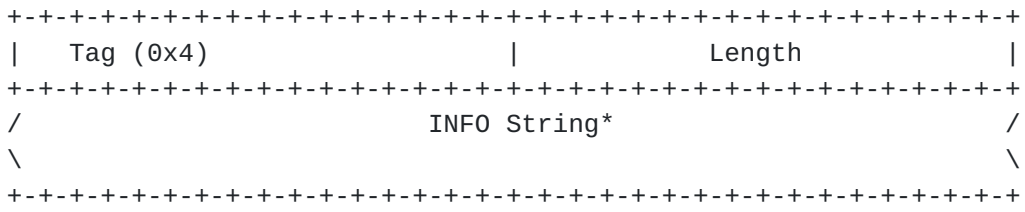
The NAASP message is sent by the SG when there are no active ASPs within an AS. The determination on whether to send a NAASP message occurs when an ASP moves from Active to Inactive. When this occurs, if there are no other ASPs in the active state, then the NAASP message is sent to every ASP defined within the AS.

The NAASP message contains the following parameters:

AS Definition (Mandatory)
INFO String (Optional)

The format for the NAASP message parameters is as follows:





The format of the AS Definition field is implementation-dependent, and therefore is specific to individual configurations. This field is an

unstructured text string that carries the AS name and its associated ASPs.

The following is an example.

```
AS Definition string
{
  AS: boston_region
  {
    ASP1:  primary segment1
    ASP2:  backup segment1
    ASP3:  primary segment2
    ASP4:  backup segment2
    ...
  }
}
```

2.6 Management Messages

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

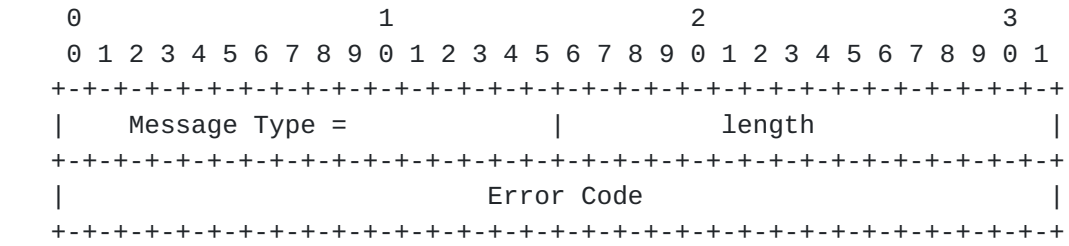
2.6.1 Error (ERR)

The ERR message is sent when an invalid value is found in an incoming message.

The ERR message contains the following parameters:

Error Code

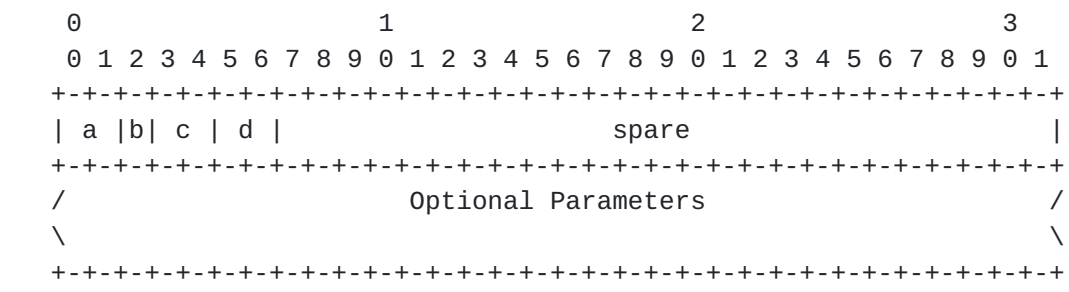
The format for the ERR message is as follows:



The Error Code can be one of the following values:

Invalid Version	0x1
Invalid Network Appearance	0x2
Invalid SCN Version	0x3
Invalid Adaptation Layer Identifier	0x4
Invalid Stream Identifier	0x5
Invalid Message Type	0x6

2.6.2 Audit



Flags

A	class
B	priority
C	ack
D	segmentation

The class flag indicates which SCCP class this data transfer is supporting. The valid values for class are shown in the following table.

Value	Description
0x0	Class 0 (connectionless service)
0x1	Class 1 (connectionless service)
0x2	Class 2 (connection-oriented service)
0x3	Class 3 (connection-oriented service)

The priority flag MUST be set to 0.

The acknowledge flag MUST be set to 0.

The segmentation flag MUST be set to 0.

Optional parameters include:

- sending address
- destination address

Implementation note:

This message covers the following SCCP messages: inactivity test (IT), subsystem-status-test (SST).

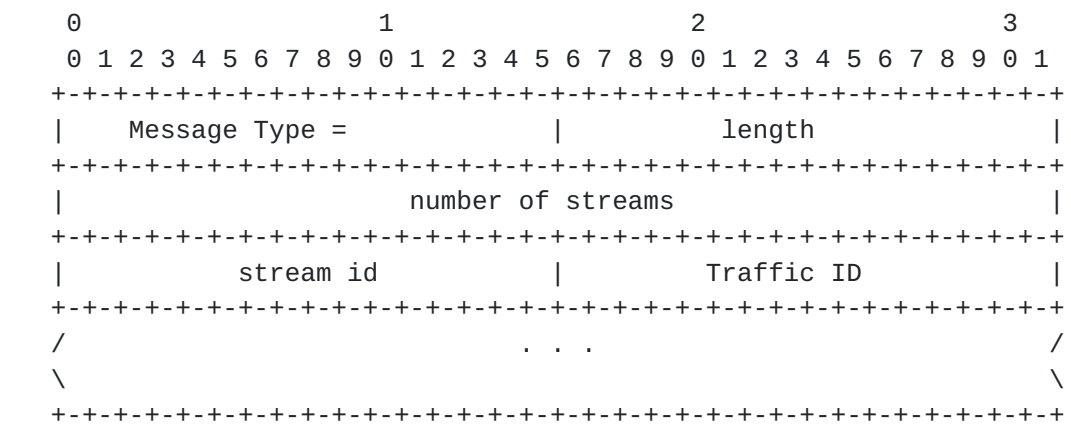
2.6.3 Stream Configuration

The Stream Configuration message allows for an ASP to indicate what which streams are supported and what range of traffic they can handle. Traffic ID is a locally configured variable, it has only local significance. It must be configured in the ASP and in the SG. A value of 0 indicates that any traffic may be supported on the stream.

The SCO message contains the following parameters:

- Number of Streams
- Stream ID
- Traffic ID

The format for the SCO message is as follows:



2.6.4 Stream Configuration Ack

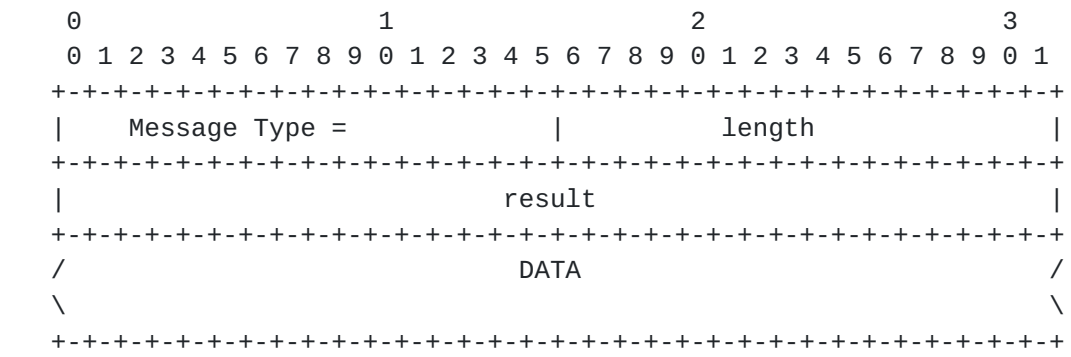
The Stream Configuration Ack message acknowledges the Stream Configuration message.

The SCA message contains the following parameters:

- Number of Streams
- Stream ID
- Traffic ID

The format for the SCO message is as follows:

- Result
- Data (optional)



The Result parameter can be one of the following values:

Success	0x0
Failure	0x1

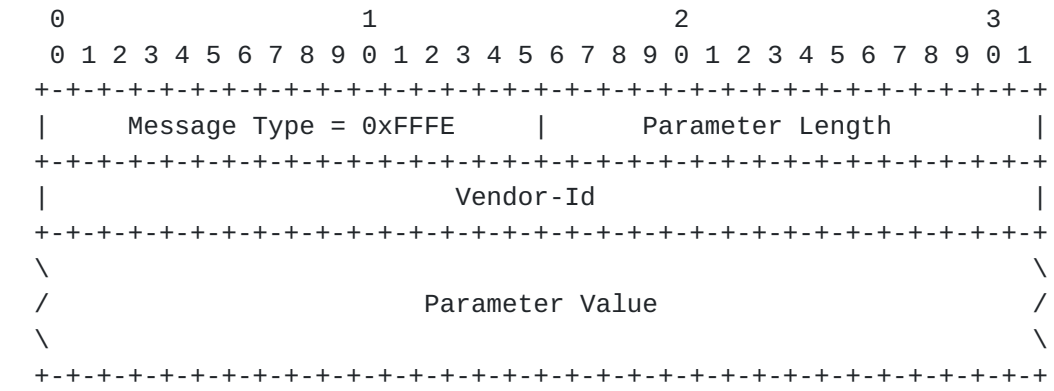
The Data parameter contains a list of stream IDs and Traffic IDs that the SG can support.

2.7 Vendor Specific Message

This is to allow vendors to support their own extended message not defined by the IETF. It MUST not affect the operation of the SUA.

Endpoints not equipped to interpret the vendor-specific messages sent by a remote endpoint MUST ignore it (although it may be reported). Endpoints that do not receive desired vendor-specific information SHOULD make an attempt to operate without it, although they may do so (and report they are doing so) in a degraded mode.

A summary of the Vendor-specific extension format is shown below. The fields are transmitted from left to right.



Type: 16 bit u_int

0xFFFE for all Vendor-Specific parameters.

Length: 16 bit u_int

Indicate the size of the parameter in octets, including the Type, Length, Vendor-Id, and Value fields.

Vendor-Id: 32 bit u_int

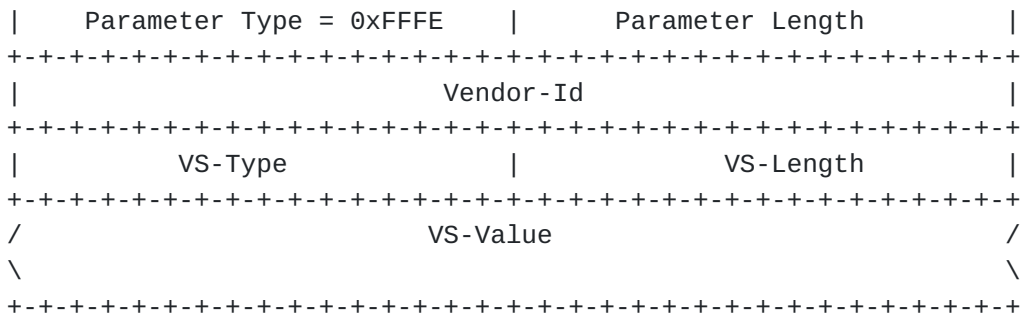
The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the Assigned Numbers (RFC 1700).

Value: variable length

The Value field is one or more octets. The actual format of the information is site or application specific, and a robust implementation SHOULD support the field as undistinguished octets.

The codification of the range of allowed usage of this field is outside the scope of this specification.

It SHOULD be encoded as a sequence of vendor type / vendor length / value fields, as follows. The parameter field is dependent on the vendor's definition of that attribute. An example encoding of the Vendor-Specific attribute using this method follows:


Parameter Type = 0xFFFE
Parameter Length
Vendor-Id
VS-Type
VS-Length
VS-Value

VS-Type: 16 bit u_int

This field identifies the parameter included in the VS-Value field. It is assigned by the vendor.

VS-Length: 16 bit u_int

This field is the length of the vendor-specific parameter and Includes the VS-Type, VS-Length and VS-Value (if included) fields.

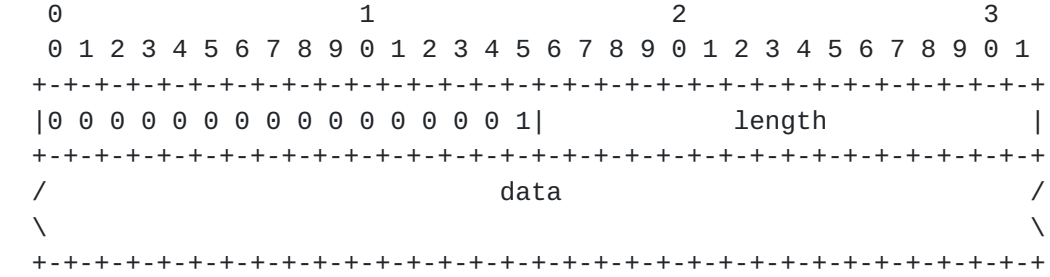
VS-Value: Variable Length

This field contains the parameter identified by the VS-Type field. It's meaning is identified by the vendor.

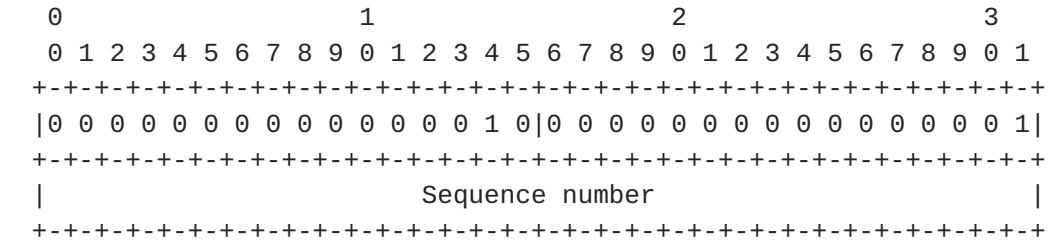
2.8 Paramters

Parameter Name	Parameter ID
Data	0x0001
Sequence Number	0x0002
Source Reference Number	0x0003
Destination Reference Number	0x0004
Source Address	0x0005
Destination Address	0x0006
Cause	0x0007

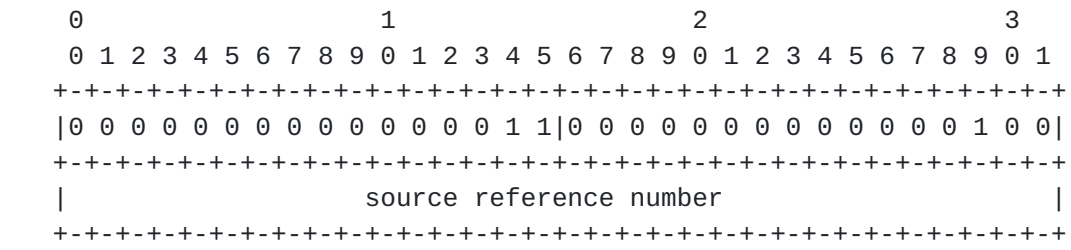
2.8.1 Data



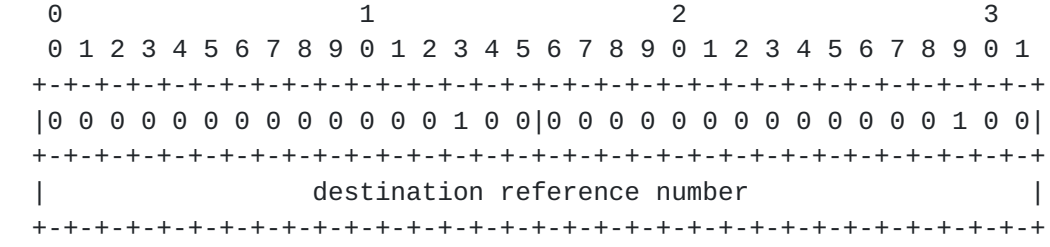
2.8.2 Sequence Number



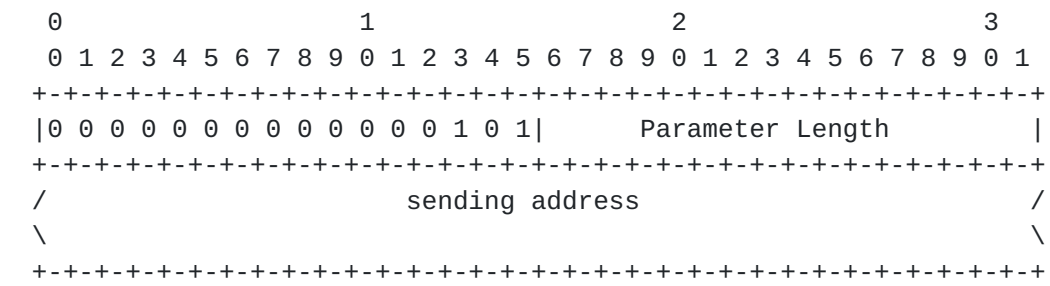
2.8.3 Source Reference Number


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
|0 0 0 0 0 0 0 0 0 0 0 0 0 1 1|0 0 0 0 0 0 0 0 0 0 0 0 1 0 0|
source reference number

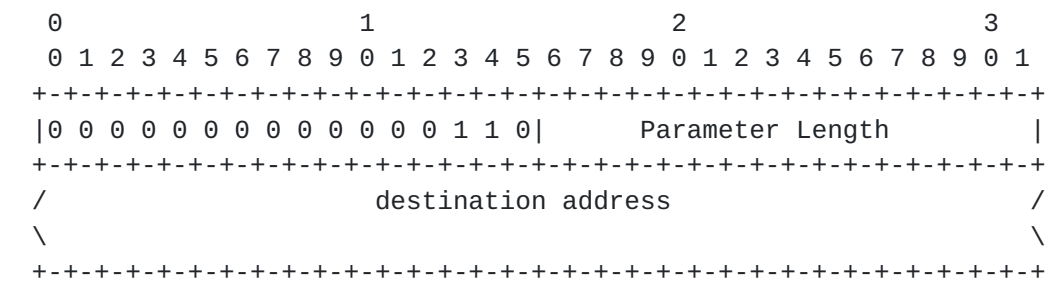
2.8.4 Destination Reference Number



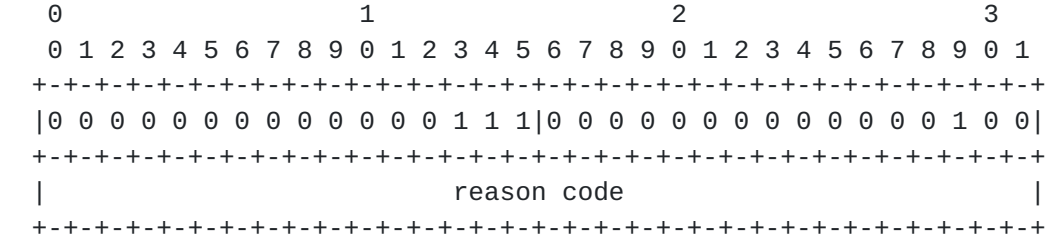
2.8.5 Sending Address



2.8.6 Destination Address



2.8.7 Cause



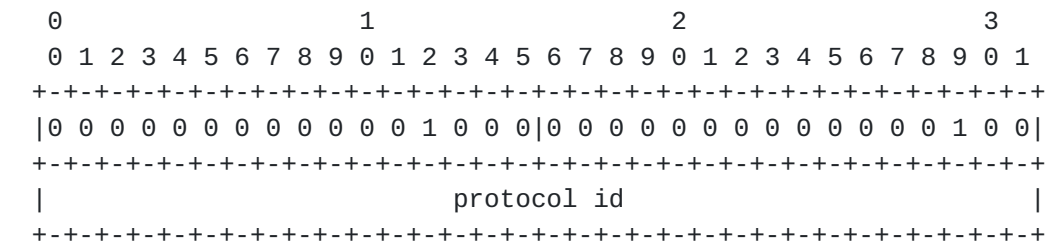
Reason code may be one of the following reasons:

Invalid Version	0x1
Invalid Network Appearance	0x2
Invalid SCN Version	0x3
Invalid Adaptation Layer Identifier	0x4
Invalid Stream Identifier	0x5

Invalid Message Type	0x6

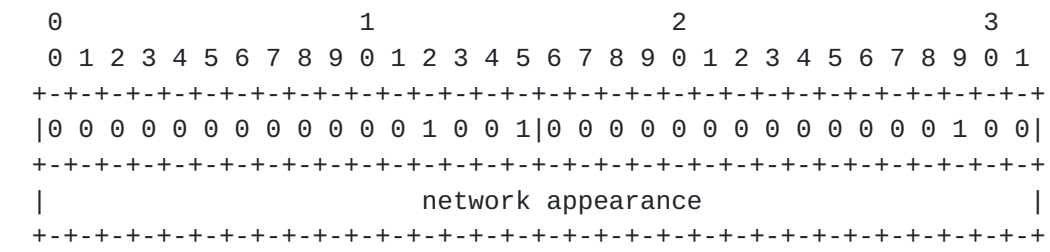
2.8.8 Protocol Identifier

The Protocol Identifier parameter identifies the SCCP version/variant.



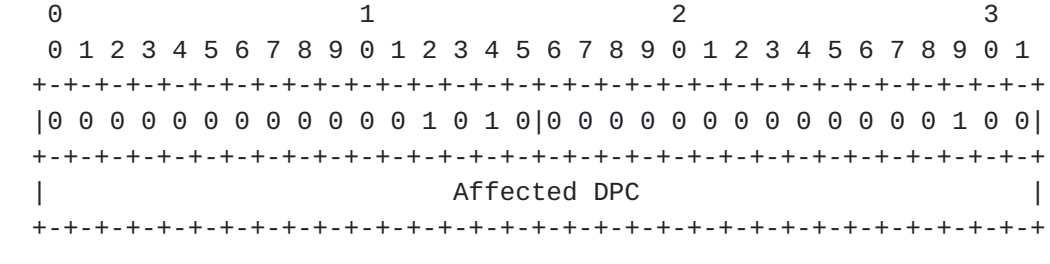
2.8.9 Network Appearance

The Network Appearance parameter identifies the SS7 network context for the message, for the purposes of logically separating the signaling traffic between the SG and the Application Server Processes over common SCTP Associations. An example is where an SG is logically partitioned to appear as an element in four different national SS7 networks. A Network Appearance implicitly defines the SS7 Destination Point Code used, the SS7 Network Indicator value and SCCP/SCCP-User protocol type/variant/version used within the SS7 network partition. Where an SG operates in the context of a single SS7 network, or individual SCTP associations are dedicated to each SS7 network appearance, the Network Appearance parameter is not required.



2.8.10 Affected Destination Point Code

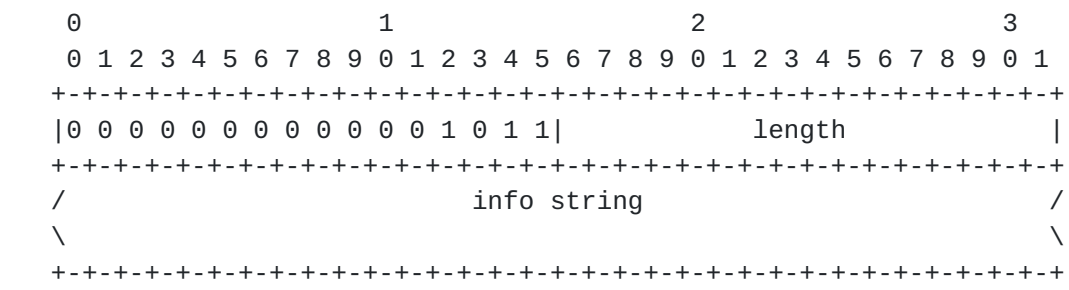
The Affected DPC is provisionally a three-octet parameter to allow 14-, 16- and 24-bit binary formatted SS7 Point Codes. Where the Affected Point Code is less than 24-bits, it is padded on the left to the 24-bit boundary.



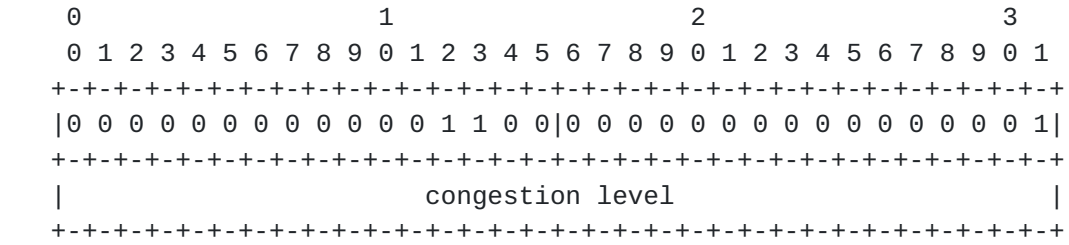
2.8.11 Info String

The INFO String parameter can carry any meaningful 8-BIT ASCII character

string along with the message. Length of the INFO String parameter is from 0 to 255 characters. No procedures are presently identified for its use but the INFO String may be used by Operators for debugging purposes.



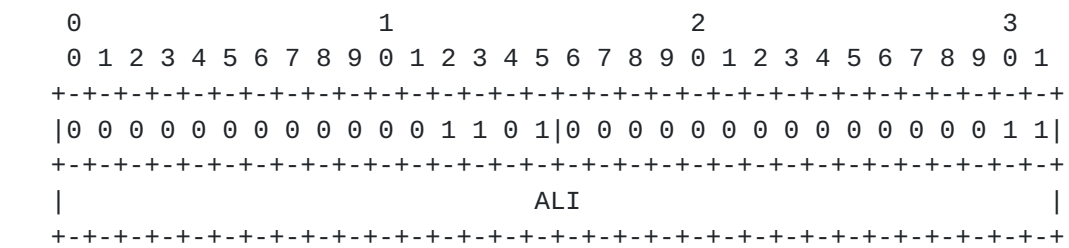
2.8.12 Congestion Level



The valid values for the optional Congestion Level parameter are shown in the following table.

Value	Description
00	No Congestion or Undefined
01	Congestion Level 1
02	Congestion Level 2
03	Congestion Level 3

2.8.13 Adaptation Layer Identifier



The optional Adaptation Layer Identifier (ALI) is a string that identifies the adaptation layer. This string MUST be set to "SUA" which results in a length of 3. The ALI would normally only be used in the initial ASP Up message across a new SCTP association to ensure both peers are assuming the same adaptation layer protocol.

3 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 layers. This section describes the SCU procedures in response to

these events.

3.1 Procedures to support the SUA Services

These procedures support the SUA transport of SCCP-User/SCCP boundary primitives.

3.1.1 Receipt of Local primitives

3.2 Procedures to support the SUA Layer Management Services

3.2.1 Layer Management primitives procedures

3.2.2 Receipt of Peer Management messages

3.3 Procedures to support the SUA SCTP Management Services

These procedures support the SUA management of SCTP Associations and ASP Paths between SGs and ASPs

3.3.1 State Maintenance

The M3UA layer on the SG needs to maintain the state of each ASP as input to the SGs address translation and mapping function.

3.3.1.1 ASP States

The state of each ASP is maintained in the M3UA layer in the SG. The state of an ASP changes due to events. The events include:

* Reception of messages from that ASP's M3UA layer
* Reception of messages from a different ASP's M3UA layer
* Reception of indications from the SCTP layer
* Switch over timer triggers

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

ASP-DOWN: The Application Server Process is unavailable. Initially all ASPs will be in this state.

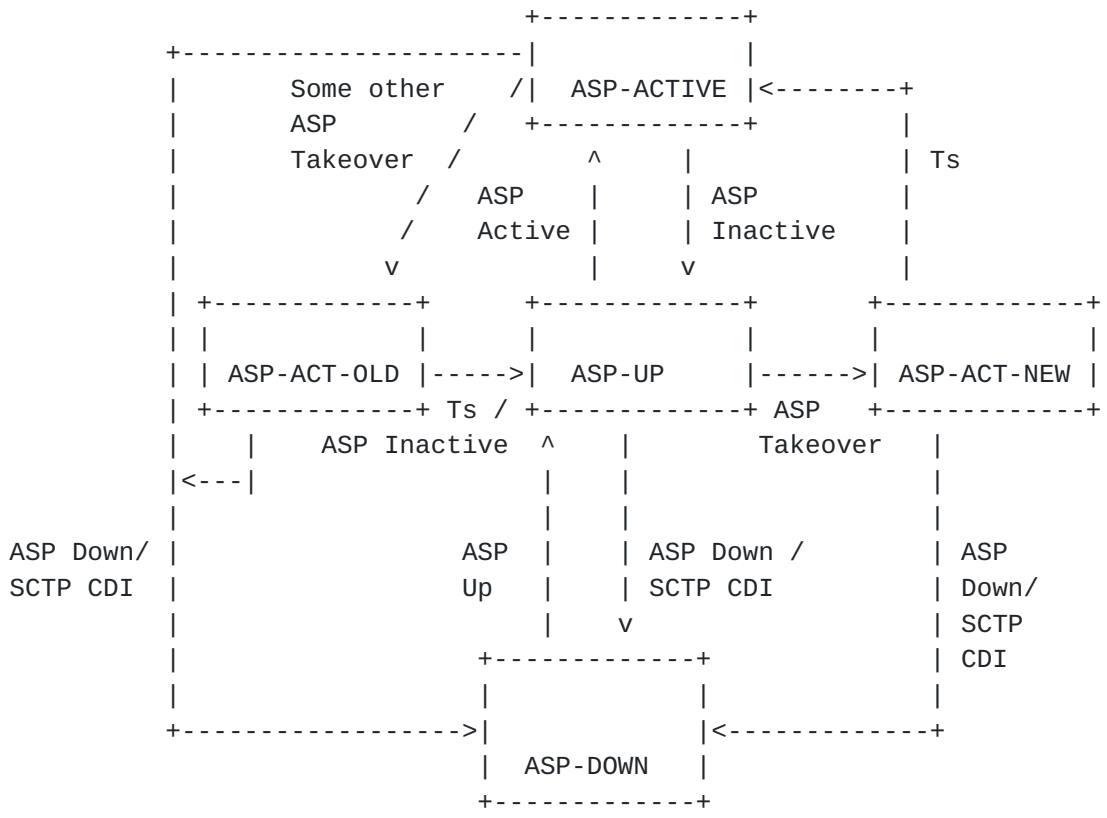
ASP-UP: The Application Server Process is available but application traffic is stopped.

ASP-ACTIVE: The Application Server Process is available and application traffic is active.

ASP-ACT-OLD: The Application Server Process is available and application traffic is active for continued work only.

ASP-ACT-NEW: The Application Server Process is available and application traffic is active for new work only.

Figure 4: ASP State Transition Diagram



SCTP CDI: The local SCTP layer's Communication Down Indication to the Upper Layer Protocol (M3UA) on an SG. The local SCTP will send this indication when it detects the loss of connectivity to the ASP's SCTP layer.

Ts: Switch over Timer Triggers

3.3.1.2 AS States

The state of the AS is maintained in the M3UA layer on the SG.

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.

AS-UP: The Application Server is available but no application traffic is active (i.e., one or more related ASPs are in the ASP-UP state, but none in the ASP-Active state).

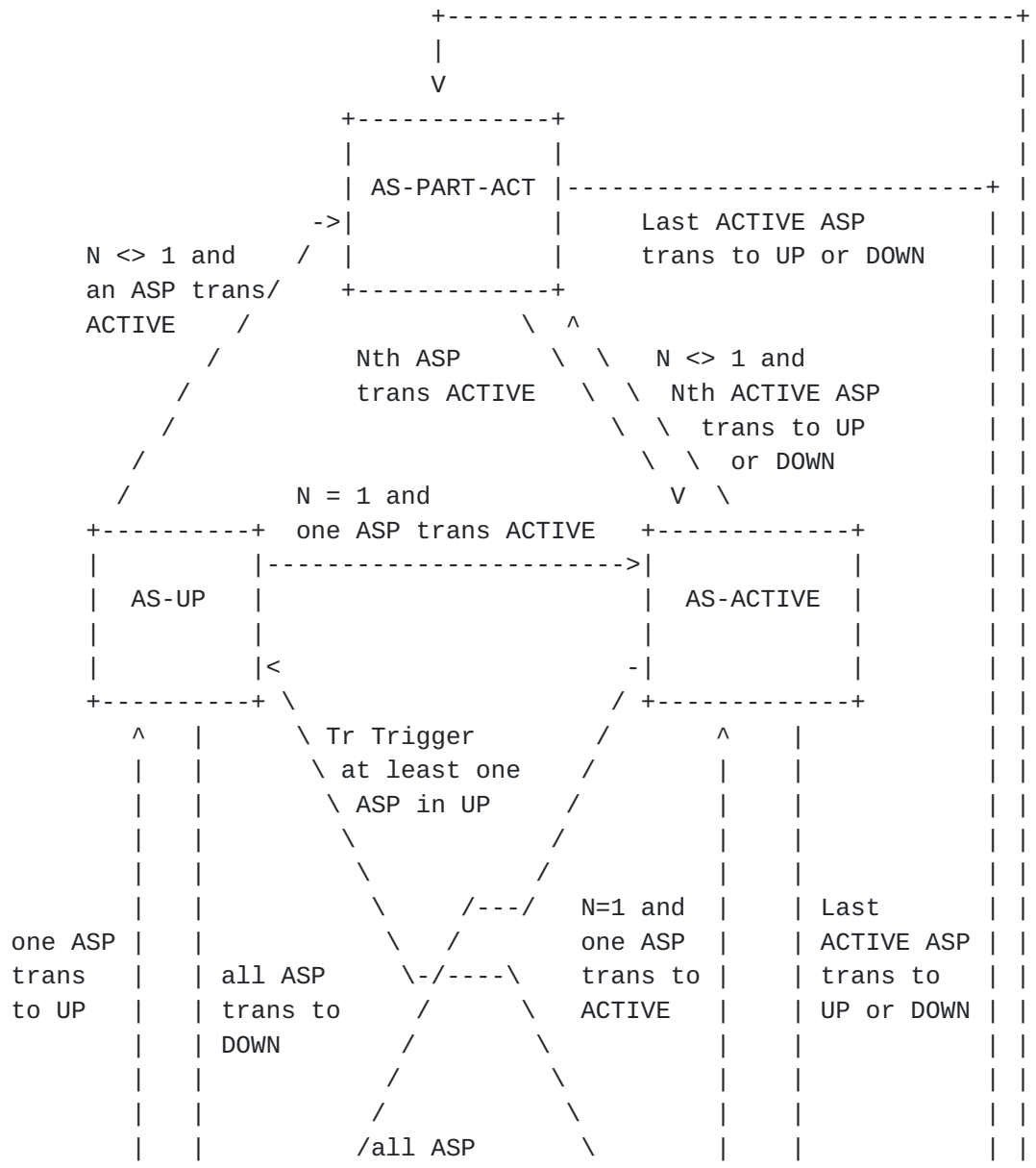
AS-ACTIVE: The Application Server is available and application traffic is active. This state implies that one ASP is in the ASP-ACTIVE state.

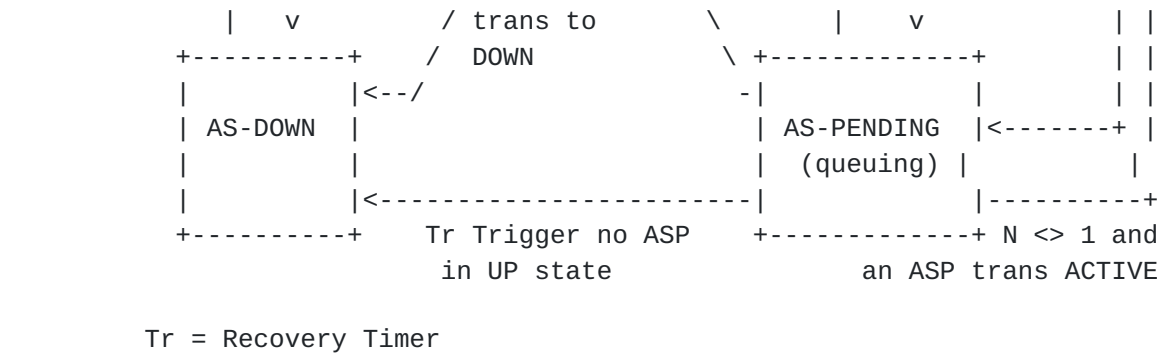
AS-PENDING: An active ASP has transitioned from active to inactive or down and it was the last remaining active ASP in the AS. A recovery

timer T(r) will be started and all incoming SCN messages will be queued by the SG. If an ASP becomes active before T(r) expires, the AS will move to AS-ACTIVE state and all the queued messages will be sent to the active ASP.

If T(r) expires before an ASP becomes active, the SG stops queuing messages and discards all previously queued messages. The AS will move to AS-UP if at least one ASP is in ASP-UP state, otherwise it will move to AS-DOWN state.

Figure 5: AS State Transition Diagram





Tr = Recovery Timer

3.3.2 ASPM procedures for primitives

Before the establishment of an SCTP association the ASP state at both the SG and ASP is assumed to be "Down".

When the SUA layer receives an M-SCTP ESTABLISH request primitive from the Layer Management, the SUA layer will try to establish an SCTP association with the remote SUA peer. Upon reception of an eventual SCTP-Communication Up confirm primitive from the SCTP, the SUA layer will invoke the primitive M-SCTP ESTABLISH confirm to the Layer Management.

Alternatively, if the remote SUA-peer establishes the SCTP association first, the SUA layer will receive an SCTP Communication Up indication primitive from the SCTP. The SUA layer will then invoke the primitive M-SCTP ESTABLISH indication to the Layer Management.

Once the SCTP association is established, The SUA layer at an ASP will then find out the state of its local SUA-user from the Layer Management using the primitive M-ASP STATUS. Based on the status of the local SUA-User, the local ASP SUA Application Server Process Maintenance (ASPM) function will initiate the ASPM procedures, using the ASP-Up/-Down/-Active/-Inactive messages to convey the ASP-state to the SG - see Section 3.3.3.

If the SUA layer subsequently receives an SCTP-Communication Down indication 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 "Down" at both the SG and ASP.

At an ASP, the Layer Management may try to reestablish the SCTP association using M-SCTP ESTABLISH request primitive.

3.3.3 ASPM procedures for peer-to-peer messages

3.3.3.1 ASP-Up

The SG will mark the path as up if an explicit ASP UP (ASPUP) message is received and internally the path is allowed to come up (i.e., not in a locked local maintenance state). An ASP UP (ASPUP) message will be sent to acknowledge the received ASPUP. The SG will respond to a ASPUP with a ASPDN message if the path is in a locked maintenance state.

The SG will send a ASPUP message in response to a received ASPUP message from the ASP even if that path was already marked as UP at the SG.

The paths are controlled by the ASP. The SG will only send ASPUP in response to the reception of a ASPUP message.

The ASP will send ASPUP messages every 2 (add text regarding this being a configurable timer) seconds until the path comes up (i.e. until it receives a ASPUP message from the SG for that path). The ASP may decide to reduce the frequency (say to every 5 seconds) if the an acknowledgement is not received after a few tries.

The ASP should wait for the ASPUP message from the SG before transmitting ASP maintenance messages (ASPIA or ASPAC) or SUA messages

or it will risk message loss. The ASPUP message received from the SG is not acknowledged by the ASP.

3.3.3.2 ASP Down

The SG will mark the ASP as down and send a ASPDN message to the ASP if one of the following events occur:

- an ASP Down(ASPDN) message is received from the ASP,
- the ASP is locked by local maintenance.

The SG will also send a ASPDN message when the ASP is already down and a ASPDN) message is received from the ASP.

The ASP will send ASPDN whenever it wants to take down a ASP. Since the ASPDN messages to the SG or the ASPDN responses from the SG can be lost (for example, during a node failover), the ASP can send ASPDN messages every 2 seconds until the path comes down (i.e. until it receives a ASPDN message from the SG for that path).

3.3.3.3 ASP Version Control

If a ASP Up message with an unknown version is received, the receiving end will respond with an Error message. This will indicate to the sender which version the receiving node supports.

This is useful when protocol version upgrades are being performed. A node with the newer version should support the older versions used on other nodes it is communicating with.

The version field in the Error message header associated will indicate the version supported by the node.

3.3.3.4 ASP Active

When an ASP Active (ASPAC) message is received, the SG will start routing to that ASP. Reception of a ASPAC message overrides any previous ASPAC messages and results in the ASP associated with the ASPAC message to become the newly active ASP.

3.3.3.5 ASP Inactive

When a ASPIA message is received, message transmission to that ASP ceases. The SG will either discard all incoming messages or start buffering the incoming messages for T(r)seconds after which messages will be discarded.

If the ASP is down, all of the Paths that were supported by that ASP

are, by default, down.

3.4 Procedures to support the SUA Services

3.4.1 At an SG

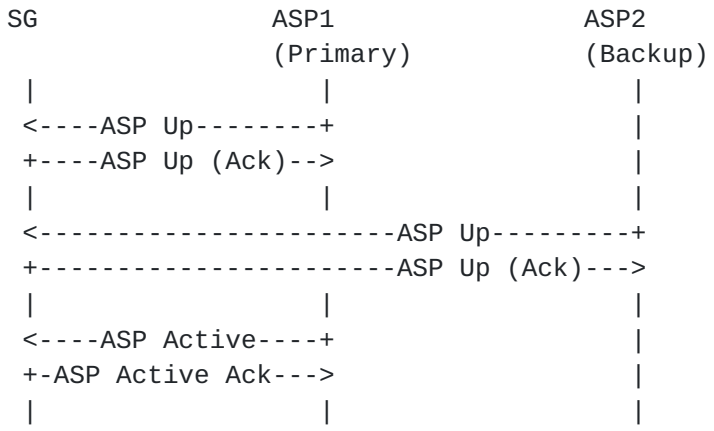
Details to be provided.

3.4.2 At an ASP

Details to be provided.

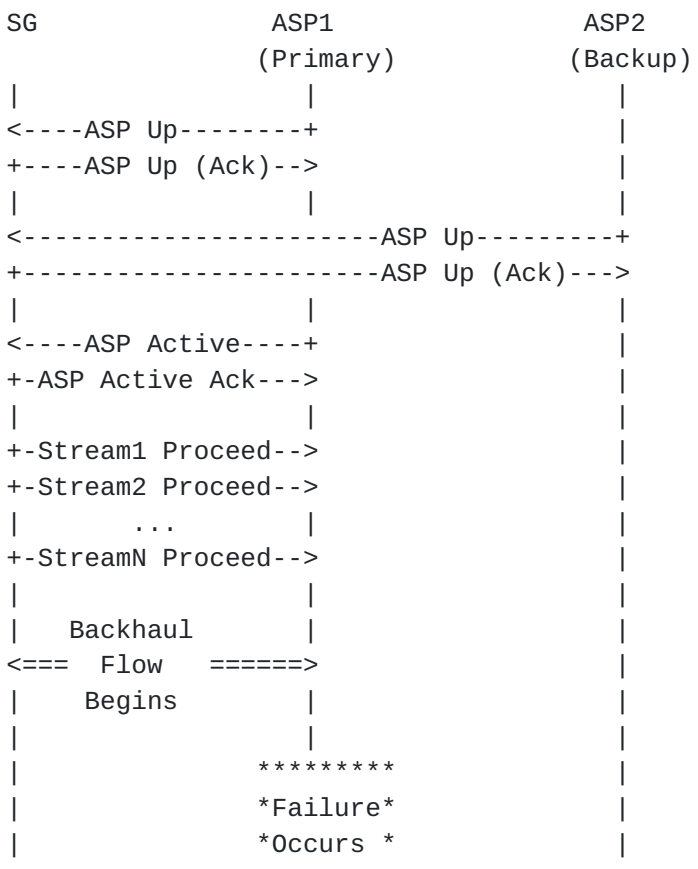
4 Examples of SUA Procedures

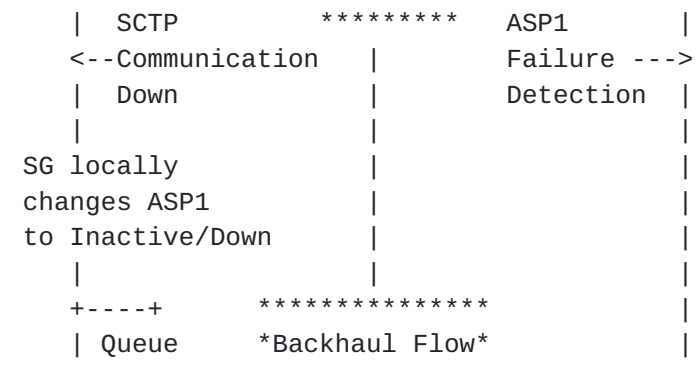
4.1 Establishment of Association

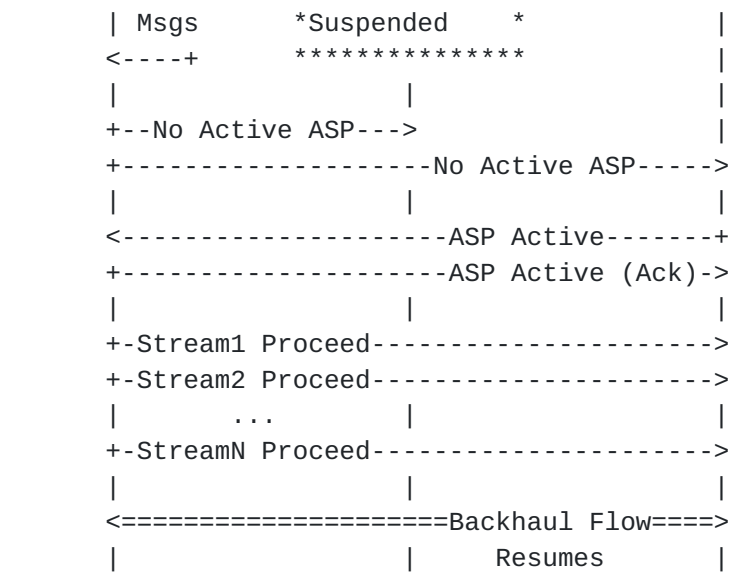


4.2 ASP fail-over Procedures

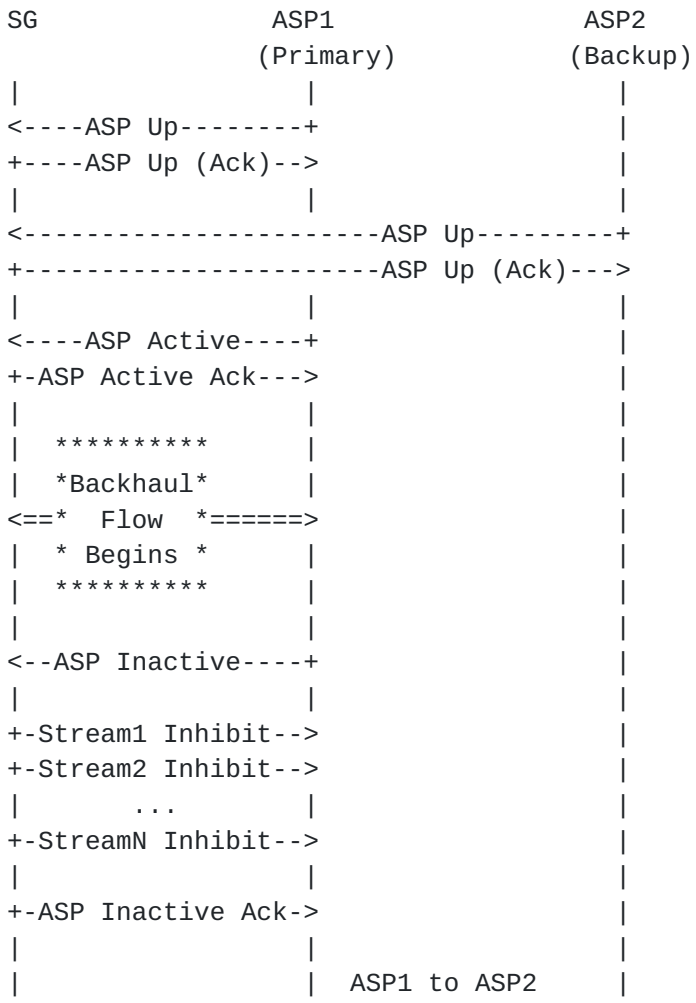
4.2.1 For Primary/Backup model

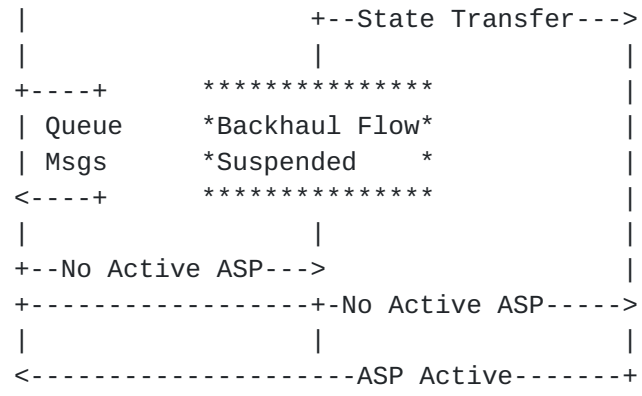


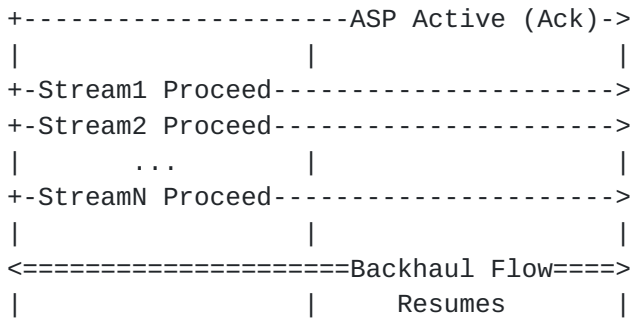

| SCTP *********
<--Communication |
| Down |
| |
SG locally |
changes ASP1 |
to Inactive/Down |
| |
+----+ **********
| Queue *Backhaul Flow*
ASP1 |
Failure --->
Detection |
|
|
|
|
|
|



4.3.2 ASP administrative switch-over for Primary/Backup model



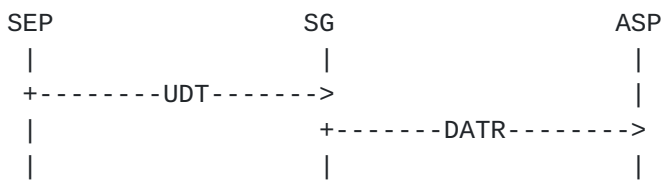

+--State Transfer--->
Queue Msgs
Backhaul Flow
Suspended
+--No Active ASP--->
+-No Active ASP----->
<----------ASP Active-------+



4.3 SUA/SCCP-User Boundary Examples

4.3.1 Data Tranfer

This is an example of data tranfer, assuming associations are already established.



5 Security

5.1 Introduction

SUA is designed to carry signaling messages for telephony services. As such, SUA must involve 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.

5.2 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 [6] 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 includes an appropriate security policy framework. The "Site Security Handbook" [11] should be consulted for guidance.

When the network in which SUA runs in involves more than one party, it may not be reasonable to expect that all parties have implemented security in a sufficient manner. In such a case, it is recommended that IPSEC is used to ensure confidentiality of user payload. Consult [9] for more information on configuring IPSEC services.

5.3 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 IANA Considerations

6.1 SCTP Protocol ID

A request will be made to IANA to assign protocol IDs. A protocol ID for the SUA will be registered.

The protocol ID is included in each SCTP data chunk, to indicate which protocol SCTP is carrying. This protocol ID is not directly used by SCTP but may be used by certain network entities to identify the type of information being carried in this DATA chunk.

6.2 Port Number

A request will be made to IANA to assign an SUA Port Number. This Port Number is the port which the SG listen to when receiving SCTP datagrams.

7 Acknowledgements

The authors would like to thank Marja-Liisa Hamalainen and Markus Maanoja for their insightful comments and suggestions.

8 Author's Addresses

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

Greg Sidebottom
Nortel Networks
3685 Richmond Rd,
Nepean, Ontario, Canada K2H 5B7

gregside@nortelnetworks.com

Guy Mousseau
Nortel Networks
3685 Richmond Rd
Nepean, Ontario, Canada K2H 5B7

Stephen Lorusso
Unisphere Solutions
200 Wheeler Road

Burlington, MA 01803
USA
SLorusso@unispheresolutions.com

9 References

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

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

[3] ANSI T1.112 'Signaling System Number 7 - Signaling Connection Control Part'

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

[5] ANSI T1.114 'Signaling System Number 7 - Transaction Capabilities Application Part'

[6] 3G TS 25.413 V3.0.0 (2000-01) 'Technical Specification 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu Interface RANAP Signalling'

[7] Simple Control Transport Protocol <draft-ietf-sigtran-sctp-05.txt>, Dec. 1999, Work in Progress

[8] MTP3-User Adaptation Layer <draft-ietf-sigtran-m3ua-01.txt>, Dec. 1999, Work in Progress

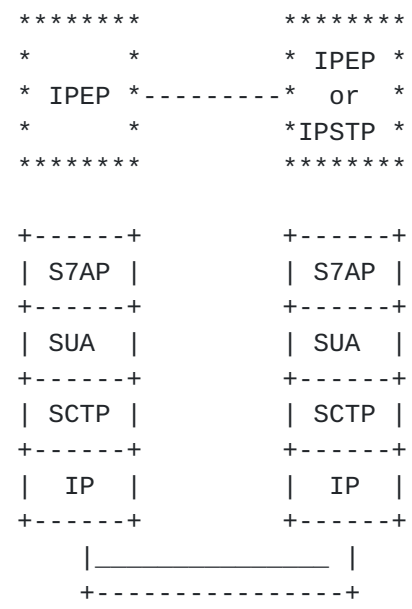
[9] RFC 2401, "Security Architecture for the Internet Protocol", S. Kent, R. Atkinson, November 1998.

[10]3G TS 25.420 V3.0.0 (2000-01) "Technical Specification 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iur Interface General Aspects and Principles"

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

ANNEX A: IP-Endpoint to IP-Endpoint Architecture

It is possible for the SUA protocol to be used between two endpoints located with an IP endpoint. In this architecture, only IP transport would be considered. This may be a likely scenario in an all IP wireless mobile network. In this architecture, the model would simplify to the figure below.



S7AP - SS7 Application Protocol (e.g. - RANAP/RNSAP)

It is possible that the IP endpoints would have connections to other hosts, for signaling transport purposes. This annex will consider possible modifications to the SUA protocol.

Details to be provided.

This draft expires September 8, 2000.