Network Working Group   Greg Sidebottom
INTERNET-DRAFT   xxx

                                                         Ken Morneault
                                                         Cisco Systems

                                                    Javier Pastor-Balbßs
                                                              Ericsson

                                                           April, 2004

Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) -
User Adaptation Layer (M3UA)
<**draft-ietf-sigtran-m3ua-v02-00.txt**>

Status of this memo

Copyright Notice

Abstract

   This memo defines a protocol for supporting the transport of any SS7
   MTP3-User signalling (e.g., ISUP and SCCP messages) over IP using the

   services of the Stream Control Transmission Protocol. Also,
   provision is made for protocol elements that enable a seamless
   operation of the MTP3-User peers in the SS7 and IP domains. This
   protocol would be used between a Signalling Gateway (SG) and a Media
   Gateway Controller (MGC) or IP-resident Database, or between two
   IP-based applications. It is assumed that the SG receives SS7
   signalling over a standard SS7 interface using the SS7 Message
   Transfer Part (MTP) to provide transport.

TABLE OF CONTENTS

Sidebottom,Morneault,Pastor   [Page 2]

1. Introduction

This memo defines a protocol for supporting the transport of any SS7
MTP3-User signalling (e.g., ISUP and SCCP messages) over IP using the
services of the Stream Control Transmission Protocol [17]. Also,
provision is made for protocol elements that enable a seamless
operation of the MTP3-User peers in the SS7 and IP domains. This
protocol would be used between a Signalling Gateway (SG) and a Media
Gaway Controller (MGC) or IP-resident Database [11], or between two
IP-based applications.

1.1 Scope

There is a need for Switched Circuit Network (SCN) signalling
protocol delivery from an SS7 Signalling Gateway (SG) to a Media
Gateway Controller (MGC) or IP-resident Database as described in the
Framework Architecture for Signalling Transport [11]. The delivery
mechanism should meet the following criteria:

* Support for the transfer of all SS7 MTP3-User Part messages (e.g.,
  ISUP [1,2,3], SCCP [4,5,6], TUP [12], etc.)
* Support for the seamless operation of MTP3-User protocol peers
* Support for the management of SCTP transport associations and
  traffic between an SG and one or more MGCs or IP-resident
  Databases
* Support for MGC or IP-resident Database process failover and load
  sharing
* Support for the asynchronous reporting of status changes to
  management

In simplistic transport terms, the SG will terminate SS7 MTP2 and
MTP3 protocol layers [7,8,9] and deliver ISUP, SCCP and/or any other
MTP3-User protocol messages, as well as certain MTP network
management events, over SCTP transport associations to MTP3-User
peers in MGCs or IP-resident Databases.

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 SIO/DPC/OPC/CIC_range. Another example is a
virtual database element, handling all HLR transactions for a
particular SS7 DPC/OPC/SCCP_SSN combination. The AS contains a set
of one or more unique Application Server Processes, of which one or
more is normally actively processing traffic. Note that there is a
1:1 relationship between an AS and a Routing Key.

Application Server Process (ASP) - A process instance of an
Application Server. An Application Server Process serves as an active

or backup process of an Application Server (e.g., part of a
distributed virtual switch or database). Examples of ASPs are
processes (or process instances) of MGCs, IP SCPs or IP HLRs. An ASP
contains an SCTP endpoint and may be configured to process signalling
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.

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 M3UA in a point-to-point fashion. Conceptually, an IPSP does
not use the services of a Signalling Gateway node.

Failover - The capability to reroute 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. Failover also applies
upon the return to service of a previously unavailable Application
Server Process.

Host - The computing platform that the process (SGP, ASP or IPSP) is
running on.

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

Linkset - A number of signalling links that directly interconnect two
signalling points, which are used as a module.

MTP - The Message Transfer Part of the SS7 protocol.

MTP3 - MTP Level 3, the signalling network layer of SS7

MTP3-User - Any protocol normally using the services of the SS7 MTP3
(e.g., ISUP, SCCP, TUP, etc.).

Network Appearance - The Network Appearance is a M3UA local reference
shared by SG and AS (typically an integer) that together with an
Signaling Point Code uniquely identifies an SS7 node by indicating
the specific SS7 network it belongs to. It can be used to distinguish
between signalling traffic associated with different networks being
sent between the SG and the ASP over a common SCTP association. An
example scenario is where an SG appears as an element in multiple
separate national SS7 networks and the same Signaling Point Code
value may be reused in different networks.

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

Routing Key - A Routing Key describes a set of SS7 parameters and parameter values that uniquely define the range of signalling traffic to be handled by a particular Application Server. Parameters within the Routing Key cannot extend across more than a single Signalling Point Management Cluster.

Routing Context - A value that uniquely identifies a Routing Key. Routing Context values are either configured using a configuration management interface, or by using the routing key management procedures defined in this document.

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

Signalling Gateway - An SG is a signaling agent that receives/sends SCN native signaling at the edge of the IP network [11]. An SG appears to the SS7 network as an SS7 Signalling Point. An SG contains a set of one or more unique Signalling Gateway Processes, of which one or more is normally actively processing traffic. 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.

Signalling Process - A process instance that uses M3UA to communicate with other signalling processes. An ASP, an SGP and an IPSP are all signalling processes.

Signalling Point Management Cluster (SPMC) - The complete set of Application Servers represented to the SS7 network under a single MTP entity (Signalling Point) in one specific Network Appearance. SPMCs are used to aggregate the availability, congestion, and user part status of an MTP entity (Signalling Point) that is distributed in the IP domain, for the purpose of supporting MTP3 management procedures towards the SS7 network. In some cases, the SG itself may also be a member of the SPMC. In this case, the SG availability /congestion /User_Part status should also be taken into account when considering any supporting MTP3 management actions.

Stream - A stream refers to an SCTP stream; a unidirectional 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 unordered delivery service.

1.3 M3UA Overview

1.3.1 Protocol Architecture

The framework architecture that has been defined for SCN signalling

transport over IP [11] uses multiple components, including a common
signalling transport protocol and an adaptation module to support the

services expected by a particular SCN signalling protocol from its
underlying protocol layer.

Within the framework architecture, this document defines an MTP3-User
adaptation module suitable for supporting the transfer of messages of
any protocol layer that is identified to the MTP Level 3 as an MTP
User. The list of these protocol layers includes, but is not limited
to, ISDN User Part (ISUP) [1,2,3], Signalling Connection Control Part
(SCCP) [4,5,6] and Telephone User Part (TUP) [12]. TCAP [13,14,15]
or RANAP [16] messages are transferred transparently by the M3UA
protocol as SCCP payload, as they are SCCP-User protocols.

It is recommended that M3UA use the services of the Stream Control
Transmission Protocol (SCTP) [17] as the underlying reliable common
signalling transport protocol. This is to take advantage of various
SCTP features such as:

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

Under certain scenarios, such as back-to-back connections without
redundancy requirements, the SCTP functions above might not be a
requirement and TCP MAY be used as the underlying common transport
protocol.

1.3.2 Services Provided by the M3UA Layer

The M3UA Layer at an ASP or IPSP provides the equivalent set of
primitives at its upper layer to the MTP3-Users as provided by the
MTP Level 3 to its local MTP3-Users at an SS7 SEP. In this way, the
ISUP and/or SCCP layer at an ASP or IPSP is unaware that the expected
MTP3 services are offered remotely from an MTP3 Layer at an SGP, and
not by a local MTP3 layer. The MTP3 layer at an SGP may also be
unaware that its local users are actually remote user parts over
M3UA. In effect, the M3UA extends access to the MTP3 layer services
to a remote IP-based application. The M3UA layer does not itself
provide the MTP3 services. However, in the case where an ASP is
connected to more than one SG, the M3UA layer at an ASP should
maintain the status of configured SS7 destinations and route messages
according to the availability and congestion status of the routes to
these destinations via each SG.

The M3UA layer may also be used for point-to-point signalling between
   two IP Server Processes (IPSPs). In this case, the M3UA layer

provides the same set of primitives and services at its upper layer
as the MTP3. However, in this case the expected MTP3 services are not
offered remotely from an SGP. The MTP3 services are provided but the
procedures to support these services are a subset of the MTP3
procedures due to the simplified point-to-point nature of the IPSP to
IPSP relationship.

1.3.2.1 Support for the Transport of MTP3-User Messages

The M3UA layer provides the transport of MTP-TRANSFER primitives
across an established SCTP association between an SGP and an ASP or
between IPSPs.

At an ASP, in the case where a destination is reachable via multiple
SGPs, the M3UA layer must also choose via which SGP the message is to
be routed or support load balancing across the SGPs, minimizing
missequencing.

The M3UA layer does not impose a 272-octet signalling information
field (SIF) length limit as specified by the SS7 MTP Level 2 protocol
[7,8,9]. Larger information blocks can be accommodated directly by
M3UA/SCTP, without the need for an upper layer segmentation/re-
assembly procedure as specified in recent SCCP or ISUP versions.
However, in the context of an SG, the maximum 272-octet block size
must be followed when interworking to a SS7 network that does not
support the transfer of larger information blocks to the final
destination. This avoids potential ISUP or SCCP fragmentation
requirements at the SGPs. The provisioning and configuration of the
SS7 network determines the restriction placed on the maximum block
size. Some configurations (e.g., Broadband MTP [21]) may permit
larger block sizes.

1.3.2.2 Native Management Functions

The M3UA layer provides the capability to indicate errors associated
with received M3UA messages and to notify, as appropriate, local
management and/or the peer M3UA.

1.3.2.3 Interworking with MTP3 Network Management Functions

At the SGP, the M3UA layer provides interworking with MTP3 management
functions to support seamless operation of the user SCN signalling
applications in the SS7 and IP domains. This includes:

- Providing an indication to MTP3-Users at an ASP that a destination
  in the SS7 network is not reachable.

- Providing an indication to MTP3-Users at an ASP that a destination
  in the SS7 network is now reachable.

- Providing an indication to MTP3-Users at an ASP that messages to a

   destination in the SS7 network are experiencing SS7 congestion.

   - Providing an indication to the M3UA layer at an ASP that the routes
     to a destination in the SS7 network are restricted.

   - Providing an indication to MTP3-Users at an ASP that a MTP3-User
     peer is unavailable.

   The M3UA layer at an ASP keeps the state of the routes to remote SS7
   destinations and may initiate an audit of the availability, the
   restricted or the congested state of remote SS7 destinations. This
   information is requested from the M3UA layer at the SGP.

   The M3UA layer at an ASP may also indicate to the SG that the M3UA
   layer itself or the ASP or the ASP's Host is congested.

1.3.2.4 Support for the Management of SCTP Associations between the SGP
and ASPs.

   The M3UA layer at the SGP maintains the availability state of all
   configured remote ASPs, to manage the SCTP Associations and the
   traffic between the M3UA peers. As well, the active/inactive and
   congestion state of remote ASPs is maintained.

   The M3UA layer MAY be instructed by local management to establish an
   SCTP association to a peer M3UA node. This can be achieved using the
   M-SCTP_ESTABLISH primitives (See Section 1.6.3 for a description of
   management primitives.) to request, indicate and confirm the
   establishment of an SCTP association with a peer M3UA node. In order
   to avoid redundant SCTP associations between two M3UA peers, one side
   (client) SHOULD be designated to establish the SCTP association, or
   M3UA configuration information maintained to detect redundant
   associations (e.g., via knowledge of the expected local and remote
   SCTP endpoint addresses).

   Local management MAY request from the M3UA layer the status of the
   underlying SCTP associations using the M-SCTP_STATUS request and
   confirm primitives. Also, the M3UA MAY autonomously inform local
   management of the reason for the release of an SCTP association,
   determined either locally within the M3UA layer or by a primitive
   from the SCTP.

   Also the M3UA layer MAY inform the local management of the change in
   status of an ASP or AS. This MAY be achieved using the M-ASP_STATUS
   request or M-AS_STATUS request primitives.

1.3.2.5 Support for the Management of Connections to Multiple SGPs

   As shown in Figure 1 an ASP may be connected to multiple SGPs. In

such a case a particular SS7 destination may be reachable via more
than one SGP and/or SG, i.e., via more than one route. As MTP3 users

only maintain status on a destination and not on a route basis, the
M3UA layer must maintain the status (availability, restriction,
and/or congestion of route to destination) of the individual routes,
derive the overall availability or congestion status of the
destination from the status of the individual routes, and inform the
MTP3 users of this derived status whenever it changes.

1.4 Functional Areas

1.4.1 Signalling Point Code Representation

For example, within an SS7 network, a Signalling Gateway might be
charged with representing a set of nodes in the IP domain into the
SS7 network for routing purposes. The SG itself, as a signalling
point in the SS7 network, might also be addressable with an SS7 Point
Code for MTP3 Management purposes. The SG Point Code might also be
used for addressing any local MTP3-Users at the SG such as a local
SCCP layer.

An SG may be logically partitioned to operate in multiple SS7 network
appearances. In such a case, the SG could be addressable with a
Point Code in each network appearance, and represents a set of nodes
in the IP domain into each SS7 network. Alias Point Codes [8] may
also be used within an SG network appearance.

Where an SG contains more than one SGP, the MTP3 routeset, SPMC and
remote AS/ASP states of each SGP SHOULD be coordinated across all the
SGPs. Rerouting of traffic between the SGPs MAY also be supported.

Application Servers can be represented under the same Point Code of
the SG, their own individual Point Codes or grouped with other
Application Servers for Point Code preservation purposes. A single
Point Code may be used to represent the SG and all the Application
Servers together, if desired.

If an ASP or group of ASPs is available to the SS7 network via more
than one SG, each with its own Point Code, the ASP(s) will typically
be represented by a Point Code that is separate from any SG Point
Code. This allows, for example, these SGs to be viewed from the SS7
network as "STPs", each having an ongoing "route" to the same ASP(s).
Under failure conditions where the ASP(s) become(s) unavailable from
one of the SGs, this approach enables MTP3 route management messaging
between the SG and SS7 network, allowing simple SS7 rerouting through
an alternate SG without changing the Destination Point Code Address
of SS7 traffic to the ASP(s).

Where a particular AS can be reached via more than one SGP, the
corresponding Routing Keys in the SGPs should be identical. (Note:
It is possible for the SGP Routing Key configuration data to be

temporarily out-of-sync during configuration updates).

```
                        +--------+
                        |        |
            +------------+  SG 1  +--------------+
  +-------+  |  SS7 links | "STP"  |  IP network  |     ----
  |  SEP  +---+           +--------+           +---/      \
  |  or   |               |*                   | ASPs  |
  |  STP  +---+           +--------+           +---\      /
  +-------+  |            |        |           |     ----
            +------------+  SG 2  +--------------+
                        | "STP"  |
                        +--------+
```

                    Figure 1   Example with mated SGs

   * Note:. SG-to-SG communication (i.e., "C-links") is recommended for
   carrier grade networks, using an MTP3 linkset or an equivalent, to
   allow rerouting between the SGs in the event of route failures. Where
   SGPs are used, inter-SGP communication might be used. Inter-SGP
   protocol is outside of the scope of this document.

   The following example shows a signalling gateway partitioned into two
   network appearances.


```
                              SG
   +-------+           +---------------+
   |  SEP  +--------------| SS7 Ntwk |M3UA|              ----
   +-------+   SS7 links |   "A"    |    |            /      \
                         |_____|    +-----------+  ASPs  |
                         |          |    |            \      /
   +-------+             | SS7 Ntwk |    |              ----
   |  SEP  +--------------+  "B"    |    |
   +-------+             +---------------+
```

                    Figure 2   Example with multiple Network

1.4.2 **Routing Contexts and Routing Keys**

1.4.2.1 **Overview**

   The distribution of SS7 messages between the SGP and the Application
   Servers is determined by the Routing Keys and their associated
   Routing Contexts. A Routing Key is essentially a set of SS7
   parameters used to filter SS7 messages, whereas the Routing Context
   parameter is a 4-byte value (integer) that is associated to that
   Routing Key in a 1:1 relationship. The Routing Context therefore can
   be viewed as an index into a sending node's Message Distribution
   Table containing the Routing Key entries.

Possible SS7 address/routing information that comprise a Routing Key
entry includes, for example, the OPC, DPC, SIO found in the MTP3

routing label. Some example Routing Keys are: the DPC alone, the
DPC/OPC combination, or the DPC/OPC/SI combination. The particular
information used to define an M3UA Routing Key is application and
network dependent, and none of the above examples are mandated.

An Application Server Process may be configured to process signalling
traffic related to more than one Application Server, over a single
SCTP Association. In ASP Active and ASP Inactive management
messages, the signalling traffic to be started or stopped is
discriminated by the Routing Context parameter. At an ASP, the
Routing Context parameter uniquely identifies the range of signalling
traffic associated with each Application Server that the ASP is
configured to receive.

1.4.2.2 Routing Key Limitations

Routing Keys SHOULD be unique in the sense that each received SS7
signalling message SHOULD have a full or partial match to a single
routing result. It is not necessary for the parameter range values
within a particular Routing Key to be contiguous.

1.4.2.3 Managing Routing Contexts and Routing Keys

There are two ways to provision a Routing Key at an SGP. A Routing
Key may be configured statically using an implementation dependent
management interface, or dynamically using the M3UA Routing Key
registration procedure.

When using a management interface to configure Routing Keys, the
message distribution function within the SGP is not limited to the
set of parameters defined in this document. Other implementation
dependent distribution algorithms may be used.

1.4.2.4 Message Distribution at the SGP

To direct messages received from the SS7 MTP3 network to the
appropriate IP destination, the SGP must perform a message
distribution function using information from the received MTP3-User
message.

To support this message distribution, the SGP might, for example,
maintain the equivalent of a network address translation table,
mapping incoming SS7 message information to an Application Server for
a particular application and range of traffic. This could be
accomplished by comparing elements of the incoming SS7 message to
currently defined Routing Keys in the SGP.

These Routing Keys could in turn map directly to an Application
Server that is enabled by one or more ASPs. These ASPs provide

dynamic status information regarding their availability, traffic
handling capability and congestion to the SGP using various

management messages defined in the M3UA protocol.

The list of ASPs in an AS is assumed to be dynamic, taking into
account the availability, traffic handling capability and congestion
status of the individual ASPs in the list, as well as configuration
changes and possible failover mechanisms.

Normally, one or more ASPs are active (i.e., currently processing
traffic) in the AS but in certain failure and transition cases it is
possible that there may be no active ASP available. Broadcast,
loadsharing and backup scenarios are supported.

When there is no matching Routing Key entry 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. The
treatment of unallocated traffic is implementation dependent.

1.4.2.5 Message Distribution at the ASP

The ASP must choose an SGP to direct a message to the SS7 network.
This is accomplished by observing the Destination Point Code (and
possibly other elements of the outgoing message such as the SLS
value). The ASP must also take into account whether the related
Routing Context is active or not (See Section 4.3.4.3).

Implementation Note: Where more than one route (or SGP) is possible
for routing to the SS7 network, the ASP could, for example, maintain
a dynamic table of available SGP routes for the SS7 destinations,
taking into account the SS7 destination
availability/restricted/congestion status received from the SGP(s),
the availability status of the individual SGPs and configuration
changes and failover mechanisms. There is, however, no M3UA messaging
to manage the status of an SGP (e.g., SGP-Up/Down/Active/Inactive
messaging).

Whenever an SCTP association to an SGP exists, the SGP is assumed to
be ready for the purposes of responding to M3UA ASPSM messages (Refer
to Section 3).

1.4.3 SS7 and M3UA Interworking

In the case of SS7 and M3UA interworking, the M3UA adaptation layer
is designed to provide an extension of the MTP3 defined user
primitives.

1.4.3.1 Signalling Gateway SS7 Layers

The SG is responsible for terminating MTP Level 3 of the SS7
protocol, and offering an IP-based extension to its users.

From an SS7 perspective, it is expected that the Signalling Gateway
transmits and receives SS7 Message Signalling Units (MSUs) to and
from the PSTN over a standard SS7 network interface, using the SS7
Message Transfer Part (MTP) [7,8,9] to provide reliable transport of
the messages.

As a standard SS7 network interface, the use of MTP Level 2
signalling links is not the only possibility. ATM-based High Speed
Links can also be used with the services of the Signalling ATM
Adaptation Layer (SAAL) [18,19].

Note: It is also possible for IP-based interfaces to be present,
using the services of the MTP2-User Adaptation Layer (M2UA) [27] or
M2PA [28].

These could be terminated at a Signalling Transfer Point (STP) or
Signalling End Point (SEP). Using the services of MTP3, the SG could
be capable of communicating with remote SS7 SEPs in a quasi-
associated fashion, where STPs may be present in the SS7 path between
the SEP and the SG.

1.4.3.2 SS7 and M3UA Interworking at the SG

The SGP provides a functional interworking of transport functions
between the SS7 network and the IP network by also supporting the
M3UA adaptation layer. It allows the transfer of MTP3-User
signalling messages to and from an IP-based Application Server
Process where the peer MTP3-User protocol layer exists.

For SS7 user part management, it is required that the MTP3-User
protocols at ASPs receive indications of SS7 signalling point
availability, SS7 network congestion, and remote User Part
unavailability as would be expected in an SS7 SEP node. To
accomplish this, the MTP-PAUSE, MTP-RESUME and MTP-STATUS indication
primitives received at the MTP3 upper layer interface at the SG need
to be propagated to the remote MTP3-User lower layer interface at the
ASP.

MTP3 management messages (such as TFPs or TFAs received from the SS7
network) MUST NOT be encapsulated as Data message Payload Data and
sent either from SG to ASP or from ASP to SG. The SG MUST terminate
these messages and generate M3UA messages as appropriate.

1.4.3.3 Application Server

A cluster of application servers is responsible for providing the
overall support for one or more SS7 upper layers. From an SS7
standpoint, a Signalling Point Management Cluster (SPMC) provides

complete support for the upper layer service for a given point code.
As an example, an SPMC providing MGC capabilities could provide

   complete support for ISUP (and any other MTP3 user located at the
   point code of the SPMC) for a given point code.

   In the case where an ASP is connected to more than one SGP, the M3UA
   layer must maintain the status of configured SS7 destinations and
   route messages according to availability/congestion/restricted status
   of the routes to these SS7 destinations.

1.4.3.4 IPSP Considerations

   Since IPSPs use M3UA in a point-to-point fashion, there is no concept
   of routing of messages beyond the remote end. Therefore, SS7 and
   M3UA interworking is not necessary for this model.

1.4.4 Redundancy Models

1.4.4.1 Application Server Redundancy

   All MTP3-User messages (e.g., ISUP, SCCP) which match a provisioned
   Routing Key at an SGP are mapped to an Application Server.

   The Application Server is the set of all ASPs associated with a
   specific Routing Key. Each ASP in this set may be active, inactive or
   unavailable. Active ASPs handle traffic; inactive ASPs might be used
   when active ASPs become unavailable.

   The failover model supports an "n+k" redundancy model, where "n" ASPs
   is the number of redundant ASPs required to handle traffic and "k"
   ASPs are available to take over for a failed or unavailable ASP.
   Traffic SHOULD be sent after "n" ASPs are active. "k" ASPs MAY be
   either active at the same time as "n" or kept inactive until needed
   due to a failed or unavailable ASP.

   A "1+1" active/backup redundancy is a subset of this model. A
   simplex "1+0" model is also supported as a subset, with no ASP
   redundancy.

1.4.5 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.

1.4.6 Congestion Management

   The M3UA 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 M3UA layer indicates congestion to local
MTP3-Users by means of an MTP-STATUS primitive, as per current MTP3
procedures, to invoke appropriate upper layer responses.

When an SG determines that the transport of SS7 messages to a
Signalling Point Management Cluster (SPMC) is encountering
congestion, the SG MAY trigger SS7 MTP3 Transfer Controlled
management messages to originating SS7 nodes, per the congestion
procedures of the relevant MTP3 standard. The triggering of SS7 MTP3
Management messages from an SG is an implementation-dependent
function.

The M3UA layer at an ASP or IPSP MAY indicate local congestion to an
M3UA peer with an SCON message. When an SG receives a congestion
message (SCON) from an ASP, and the SG determines that an SPMC is now
encountering congestion, it MAY trigger SS7 MTP3 Transfer Controlled
management messages to concerned SS7 destinations according to
congestion procedures of the relevant MTP3 standard.

1.4.7 **SCTP Stream Mapping.**

The M3UA layer at both the SGP and ASP also supports the assignment
of signalling traffic into streams within an SCTP association.
Traffic that requires sequencing SHOULD be assigned to the same
stream. To accomplish this, MTP3-User traffic may be assigned to
individual streams based on, for example, the SLS value in the MTP3
Routing Label, subject of course to the maximum number of streams
supported by the underlying SCTP association.

The following rules MUST to be followed (see section 3.1.2):

1. DATA message is never sent on stream 0.
2. ASPSM, MGMT, RKM classes should be sent on stream 0 (Other than
   BEAT, BEAT ACK and NTFY messages)
3. SSNM, ASPTM classes and BEAT, BEAT ACK and NTFY messages can be
   sent on any stream.

1.4.8 **Client/Server Model**

It is recommended that the SGP and ASP be able to support both client
and server operation. The peer endpoints using M3UA SHOULD be
configured so that one always takes on the role of client and the
other the role of server for initiating SCTP associations. The
default orientation would be for the SGP to take on the role of
server while the ASP is the client. In this case, ASPs SHOULD
initiate the SCTP association to the SGP.

In the case of IPSP to IPSP communication, the peer endpoints using

M3UA SHOULD be configured so that one always takes on the role of
client and the other the role of server for initiating SCTP

associations.

The SCTP and TCP Registered User Port Number Assignment for M3UA is
2905.

1.5 Sample Configuration

1.5.1 Example 1: ISUP Message Transport

```
     ********    SS7    ****************   IP   ********
     * SEP  *---------*      SGP       *--------* ASP  *
     ********          ****************        ********


     +------+         +--------------+         +------+
     | ISUP |         |     (NIF)    |         | ISUP |
     +------+         +------+ +------+         +------+
     | MTP3 |         | MTP3 | | M3UA |         | M3UA |
     +------|         +------+-+------+         +------+
     | MTP2 |         | MTP2 | | SCTP |         | SCTP |
     +------+         +------+ +------+         +------+
     |  L1  |         |  L1  | |  IP  |         |  IP  |
     +------+         +------+ +------+         +------+
        |_____|         |_____|
```

        SEP - SS7 Signalling End Point
        SCTP - Stream Control Transmission Protocol
        NIF - Nodal Interworking Function

In this example, the SGP provides an implementation-dependent nodal
interworking function (NIF) that allows the MGC to exchange SS7
signalling messages with the SS7-based SEP. The NIF within the SGP
serves as the interface within the SGP between the MTP3 and M3UA.
This nodal interworking function has no visible peer protocol with
either the MGC or SEP. It also provides network status information
to one or both sides of the network.

For internal SGP modeling purposes, at the NIF level, SS7 signalling
messages that are destined to the MGC are received as MTP-TRANSFER
indication primitives from the MTP Level 3 upper layer interface,
translated to MTP-TRANSFER request primitives, and sent to the local
M3UA-resident message distribution function for ongoing routing to
the final IP destination. Messages received from the local M3UA
network address translation and mapping function as MTP-TRANSFER
indication primitives are sent to the MTP Level 3 upper layer
interface as MTP-TRANSFER request primitives for ongoing MTP Level 3
routing to an SS7 SEP. For the purposes of providing SS7 network
status information the NIF also delivers MTP-PAUSE, MTP-RESUME and
MTP-STATUS indication primitives received from the MTP Level 3 upper

layer interface to the local M3UA-resident management function. In
addition, as an implementation and network option, restricted

destinations are communicated from MTP network management to the
local M3UA-resident management function.

1.5.2 **Example 2: SCCP Transport between IPSPs**

```
        ********     IP     ********
        * IPSP *            * IPSP *
        ********            ********


        +------+            +------+
        |SCCP- |            |SCCP- |
        | User |            | User |
        +------+            +------+
        | SCCP |            | SCCP |
        +------+            +------+
        | M3UA |            | M3UA |
        +------+            +------+
        | SCTP |            | SCTP |
        +------+            +------+
        |  IP  |            |  IP  |
        +------+            +------+
            |_____|
```

This example shows an architecture where no Signalling Gateway is
used. In this example, SCCP messages are exchanged directly between
two IP-resident IPSPs with resident SCCP-User protocol instances,
such as RANAP or TCAP. SS7 network interworking is not required,
therefore there is no MTP3 network management status information for
the SCCP and SCCP-User protocols to consider. Any MTP-PAUSE, MTP-
RESUME or MTP-STATUS indications from the M3UA layer to the SCCP
layer should consider the status of the SCTP Association and
underlying IP network and any congestion information received from
the remote site.

1.5.3 Example 3: SGP Resident SCCP Layer, with Remote ASP

```
        ********   SS7   ****************   IP   ********
        * SEP  *---------*                *--------*      *
        *  or  *         *      SGP       *        * ASP  *
        * STP  *         *                *        *      *
        ********         ****************          ********


        +------+         +---------------+        +------+
        | SCCP-|         |     SCCP      |        | SCCP-|
        | User |         +---------------+        | User |
        +------+            |   _____   |         +------+
        | SCCP |            | |     | |           | SCCP |
        +------+         +------+-+------+         +------+
```

```
| MTP3 |         | MTP3 | | M3UA |        | M3UA |
+------|         +------+ +------+        +------+
| MTP2 |         | MTP2 | | SCTP |        | SCTP |
```

```
        +------+            +------+ +------+        +------+
        |  L1  |            |  L1  | |  IP  |        |  IP  |
        +------+            +------+ +------+        +------+
           |_____|          |_____|
```

        STP - SS7 Signalling Transfer Point

   In this example, the SGP contains an instance of the SS7 SCCP
   protocol layer that may, for example, perform the SCCP Global Title
   Translation (GTT) function for messages logically addressed to the SG
   SCCP. If the result of a GTT for an SCCP message yields an SS7 DPC
   or DPC/SSN address of an SCCP peer located in the IP domain, the
   resulting MTP-TRANSFER request primitive is sent to the local M3UA-
   resident network address translation and mapping function for ongoing
   routing to the final IP destination.

   Similarly, the SCCP instance in an SGP can perform the SCCP GTT
   service for messages logically addressed to it from SCCP peers in the
   IP domain. In this case, MTP-TRANSFER indication primitives are sent
   from the local M3UA-resident network address translation and mapping
   function to the SCCP for GTT. If the result of the GTT yields the
   address of an SCCP peer in the SS7 network then the resulting MTP-
   TRANSFER request primitive is given to the MTP3 for delivery to an
   SS7-resident node.

   It is possible that the above SCCP GTT at the SGP could yield the
   address of an SCCP peer in the IP domain and the resulting MTP-
   TRANSFER request primitive would be sent back to the M3UA layer for
   delivery to an IP destination.

   For internal SGP modeling purposes, this may be accomplished with the
   use of an implementation-dependent nodal interworking function within
   the SGP that effectively sits below the SCCP and routes MTP-TRANSFER
   request/indication messages to/from both the MTP3 and the M3UA layer,
   based on the SS7 DPC or DPC/SI address information. This nodal
   interworking function has no visible peer protocol with either the
   ASP or SEP.

   Note that the services and interface provided by the M3UA layer are
   the same as in Example 1 and the functions taking place in the SCCP
   entity are transparent to the M3UA layer. The SCCP protocol
   functions are not reproduced in the M3UA protocol.

1.6 Definition of M3UA Boundaries

1.6.1 Definition of the Boundary between M3UA and an MTP3-User.

   From ITU Q.701 [7]:

```
     MTP-TRANSFER request
     MTP-TRANSFER indication
```

        MTP-PAUSE indication
        MTP-RESUME indication
        MTP-STATUS indication

1.6.2 **Definition of the Boundary between M3UA and SCTP**

   An example of the upper layer primitives provided by the SCTP are
   provided in Reference [17] Section 10.

1.6.3 **Definition of the Boundary between M3UA and Layer Management**

      M-SCTP_ESTABLISH request
      Direction: LM -> M3UA
      Purpose: LM requests ASP to establish an SCTP association with its
      peer.

      M-STCP_ESTABLISH confirm
      Direction: M3UA -> LM
      Purpose: ASP confirms to LM that it has established an SCTP
      association with its peer.

      M-SCTP_ESTABLISH indication
      Direction: M3UA -> LM
      Purpose: M3UA informs LM that a remote ASP has established an SCTP
      association.

      M-SCTP_RELEASE request
      Direction: LM -> M3UA
      Purpose: LM requests ASP to release an SCTP association with its
      peer.

      M-SCTP_RELEASE confirm
      Direction: M3UA -> LM
      Purpose: ASP confirms to LM that it has released SCTP association
      with its peer.

      M-SCTP_RELEASE indication
      Direction: M3UA -> LM
      Purpose: M3UA informs LM that a remote ASP has released an SCTP
      Association or the SCTP association has failed.

      M-SCTP_RESTART indication
      Direction: M3UA -> LM
      Purpose: M3UA informs LM that an SCTP restart indication has been
      received.

      M-SCTP_STATUS request
      Direction: LM -> M3UA
      Purpose: LM requests M3UA to report the status of an SCTP

association.

    M-SCTP_STATUS confirm
    Direction: M3UA -> LM
    Purpose: M3UA responds with the status of an SCTP association.

    M-SCTP STATUS indication
    Direction: M3UA -> LM
    Purpose: M3UA reports the status of an SCTP association.

    M-ASP_STATUS request
    Direction: LM -> M3UA
    Purpose: LM requests M3UA to report the status of a local or remote
    ASP.

    M-ASP_STATUS confirm
    Direction: M3UA -> LM
    Purpose: M3UA reports status of local or remote ASP.

    M-AS_STATUS request
    Direction: LM -> M3UA
    Purpose: LM requests M3UA to report the status of an AS.

    M-AS_STATUS confirm
    Direction: M3UA -> LM
    Purpose: M3UA reports the status of an AS.

    M-NOTIFY indication
    Direction: M3UA -> LM
    Purpose: M3UA reports that it has received a Notify message
    from its peer.

    M-ERROR indication
    Direction: M3UA -> LM
    Purpose: M3UA 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 -> M3UA
    Purpose: LM requests ASP to start its operation and send an ASP Up
    message to its peer.

    M-ASP_UP confirm
    Direction: M3UA -> LM
    Purpose: ASP reports that is has received an ASP UP Ack message from
    its peer.

    M-ASP_UP indication
    Direction: M3UA -> LM
    Purpose: M3UA reports it has successfully processed an incoming ASP
    Up message from its peer.

```
   M-ASP_DOWN request
```

Direction: LM -> M3UA
Purpose: LM requests ASP to stop its operation and send an ASP Down
message to its peer.

M-ASP_DOWN confirm
Direction: M3UA -> LM
Purpose: ASP reports that is has received an ASP Down Ack message
from its peer.

M-ASP_DOWN indication
Direction: M3UA -> LM
Purpose: M3UA 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 -> M3UA
Purpose: LM requests ASP to send an ASP Active message to its peer.

M-ASP_ACTIVE confirm
Direction: M3UA -> LM
Purpose: ASP reports that is has received an ASP Active
Ack message from its peer.

M-ASP_ACTIVE indication
Direction: M3UA -> LM
Purpose: M3UA reports it has successfully processed an incoming ASP
Active message from its peer.

M-ASP_INACTIVE request
Direction: LM -> M3UA
Purpose: LM requests ASP to send an ASP Inactive message to its
peer.

M-ASP_INACTIVE confirm
Direction: LM -> M3UA
Purpose: ASP reports that is has received an ASP Inactive
Ack message from its peer.

M-ASP_INACTIVE indication
Direction: M3UA -> LM
Purpose: M3UA reports it has successfully processed an incoming ASP
Inactive message from its peer.

M-AS_ACTIVE indication
Direction: M3UA -> LM
Purpose: M3UA reports that an AS has moved to the AS-ACTIVE state.

M-AS_INACTIVE indication

Direction: M3UA -> LM
     Purpose: M3UA reports that an AS has moved to the AS-INACTIVE state.

M-AS_DOWN indication
Direction: M3UA -> LM
Purpose: M3UA reports that an AS has moved to the AS-DOWN state.

If dynamic registration of RK is supported by the M3UA layer, the
layer MAY support the following additional primitives:

M-RK_REG request
Direction: LM -> M3UA
Purpose: LM requests ASP to register RK(s) with its peer by sending
REG REQ message

M-RK_REG confirm
Direction: M3UA -> LM
Purpose: ASP reports that it has received REG RSP message with
registration status as successful from its peer.

M-RK_REG indication
Direction: M3UA -> LM
Purpose: M3UA informs LM that it has successfully processed an
incoming REG REQ message.

M-RK_DEREG request
Direction: LM -> M3UA
Purpose: LM requests ASP to deregister RK(s) with its peer by
sending DEREG REQ message.

M-RK_DEREG confirm
Direction: M3UA -> LM
Purpose: ASP reports that it has received DEREG REQ message with
deregistration status as successful from its peer.

M-RK_DEREG indication
Direction: M3UA -> LM
Purpose: M3UA 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
[20].

3. M3UA Protocol Elements

The general M3UA message format includes a Common Message Header
followed by 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 MTP3-User Adaptation require a message
header which contains the adaptation layer version, the message type,
and message length.

```
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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Version    |    Reserved     | Message Class | Message Type  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Message Length                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                                \
/                                                                /
```

All fields in an M3UA message MUST be transmitted in the network byte
order, unless otherwise stated.

3.1.1 M3UA Protocol Version: 8 bits (unsigned integer)

The version field contains the version of the M3UA adaptation layer.

The supported versions are the following:

```
    1       Release 1.0
```

3.1.2 Message Classes and Types

The following list contains the valid Message Classes:

   Message Class: 8 bits (unsigned integer)

The following list contains the valid Message Type Classes:

```
    0      Management (MGMT) Messages
    1      Transfer Messages
    2      SS7 Signalling Network Management (SSNM) Messages
    3      ASP State Maintenance (ASPSM) Messages
    4      ASP Traffic Maintenance (ASPTM) Messages
    5      Reserved for Other Sigtran Adaptation Layers
    6      Reserved for Other Sigtran Adaptation Layers
    7      Reserved for Other Sigtran Adaptation Layers
    8      Reserved for Other Sigtran Adaptation Layers
    9      Routing Key Management (RKM) Messages
  10 to 127 Reserved by the IETF
  128 to 255 Reserved for IETF-Defined Message Class extensions
```

Message Type: 8 bits (unsigned integer)

The following list contains the message types for the defined
messages.

Management (MGMT) Messages (See Section 3.8)

```
      0        Error (ERR)
      1        Notify (NTFY)
   2 to 127    Reserved by the IETF
 128 to 255    Reserved for IETF-Defined MGMT extensions
```

Transfer Messages (See Section 3.3)

```
      0        Reserved
      1        Payload Data (DATA)
   2 to 127    Reserved by the IETF
 128 to 255    Reserved for IETF-Defined Transfer extensions
```

SS7 Signalling Network Management (SSNM) Messages (See Section
3.4)

```
      0        Reserved
      1        Destination Unavailable (DUNA)
      2        Destination Available (DAVA)
      3        Destination State Audit (DAUD)
      4        Signalling Congestion (SCON)
      5        Destination User Part Unavailable (DUPU)
      6        Destination Restricted (DRST)
   7 to 127    Reserved by the IETF
 128 to 255    Reserved for IETF-Defined SSNM extensions
```

ASP State Maintenance (ASPSM) Messages (See Section 3.5)

```
      0        Reserved
      1        ASP Up (ASPUP)
      2        ASP Down (ASPDN)
      3        Heartbeat (BEAT)
      4        ASP Up Acknowledgement (ASPUP ACK)
      5        ASP Down Acknowledgement (ASPDN ACK)
      6        Heartbeat Acknowledgement (BEAT ACK)
   7 to 127    Reserved by the IETF
 128 to 255    Reserved for IETF-Defined ASPSM extensions
```

ASP Traffic Maintenance (ASPTM) Messages (See Section 3.7)

```
      0        Reserved
      1        ASP Active (ASPAC)
      2        ASP Inactive (ASPIA)
      3        ASP Active Acknowledgement (ASPAC ACK)
      4        ASP Inactive Acknowledgement (ASPIA ACK)
```

```
   5 to 127     Reserved by the IETF
 128 to 255     Reserved for IETF-Defined ASPTM extensions
```

Routing Key Management (RKM) Messages (See [Section 3.6](#))

```
     0           Reserved
     1           Registration Request (REG REQ)
     2           Registration Response (REG RSP)
     3           Deregistration Request (DEREG REQ)
     4           Deregistration Response (DEREG RSP)
   5 to 127      Reserved by the IETF
 128 to 255      Reserved for IETF-Defined RKM extensions
```

[3.1.3](#) **Reserved: 8 bits**

The Reserved field SHOULD be set to all '0's and ignored by the
receiver.

[3.1.4](#) **Message Length: 32-bits (unsigned integer)**

The Message Length defines the length of the message in octets,
including the Common Header. The Message Length MUST include
parameter padding bytes, if any.

Note: A receiver SHOULD accept the message whether or not the final
parameter padding is included in the message length.

[3.2](#) **Variable Length Parameter Format**

M3UA messages consist of a Common Header followed by zero or more
variable length parameters, as defined by the message type. All the
parameters contained in a message are defined in a Tag Length-Value
format as shown below.

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Parameter Tag        |       Parameter Length        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                       Parameter Value                         /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Where more than one parameter is included in a message, the
parameters may be in any order, except where explicitly mandated. A
receiver SHOULD accept the parameters in any order.

Unless explicitly stated or shown in a message format diagram, only
one parameter of the same type is allowed in a message.

```
Parameter Tag: 16 bits (unsigned integer)
```

The Tag field is a 16-bit identifier of the type of parameter. It
takes a value of 0 to 65534. Common parameters used by adaptation
layers are in the range of 0x00 to 0x3f.   M3UA-specific
parameters have Tags in the range 0x0200 to 0x02ff. The parameter
Tags defined are as follows:

Common Parameters. These TLV parameters are common across the
different adaptation layers:

```
Parameter Name                     Parameter ID
==============                     ============
Reserved                            0x0000
Not Used in M3UA                    0x0001
Not Used in M3UA                    0x0002
Not Used in M3UA                    0x0003
INFO String                         0x0004
Not Used in M3UA                    0x0005
Routing Context                     0x0006
Diagnostic Information              0x0007
Not Used in M3UA                    0x0008
Heartbeat Data                      0x0009
Not Used in M3UA                    0x000a
Traffic Mode Type                   0x000b
Error Code                          0x000c
Status                              0x000d
Not Used in M3UA                    0x000e
Not Used in M3UA                    0x000f
Not Used in M3UA                    0x0010
ASP Identifier                      0x0011
Affected Point Code                 0x0012
Correlation ID                      0x0013
```

M3UA-Specific parameters. These TLV parameters are specific to
the M3UA protocol:

```
Network Appearance                  0x0200
Reserved                            0x0201
Reserved                            0x0202
Reserved                            0x0203
User/Cause                          0x0204
Congestion Indications              0x0205
Concerned Destination               0x0206
Routing Key                         0x0207
Registration Result                 0x0208
Deregistration Result               0x0209
Local Routing Key Identifier        0x020a
Destination Point Code              0x020b
Service Indicators                  0x020c
```

```
        Reserved                            0x020d
        Originating Point Code List         0x020e
        Reserved                            0x020f
```

        Protocol Data   0x0210
        Reserved   0x0211
        Registration Status   0x0212
        Deregistration Status   0x0213

        Reserved by the IETF   0x0214 to 0xffff

    The value of 65535 is reserved for IETF-defined extensions.
    Values other than those defined in specific parameter description
    are reserved for use by the IETF.

  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. Thus, a parameter with a zero-length
    Parameter Value field would have a Length field of 4. The
    Parameter Length does not include any padding bytes. If the
    parameter contains subparameters, the Parameter Length field
    will include all the bytes of each subparameter including
    subparameter padding bytes (if any).

  Parameter Value: variable length.

    The Parameter Value field contains the actual information to be
    transferred 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 MUST NOT pad with more than 3
    bytes. The receiver MUST ignore the padding bytes.

3.3 Transfer Messages

  The following section describes the Transfer messages and parameter
  contents.

3.3.1 Payload Data Message (DATA)

  The DATA message contains the SS7 MTP3-User protocol data, which is
  an MTP-TRANSFER primitive, including the complete MTP3 Routing Label.
  The DATA message contains the following variable length parameters:

        Network Appearance   Conditional
        Routing Context   Conditional
        Protocol Data   Mandatory

```
      Correlation Id          Optional
```

The following format MUST be used for the Data Message:

```
 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 = 0x0200           |           Length = 8          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Network Appearance                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Tag = 0x0006           |           Length = 8          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Routing Context                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Tag = 0x0210           |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                               \
/                       Protocol Data                          /
\                                                               \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Tag = 0x0013           |           Length = 8          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Correlation Id                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Network Appearance: 32-bits (unsigned integer)

   The Network Appearance parameter identifies the SS7 network
   context for the message and implicitly identifies the used SS7
   Point Code format, the SS7 Network Indicator value, and the MTP3
   and possibly the MTP3-User protocol type/variant/version used
   within the specific SS7 network. Where a SG operates in the
   context of a single SS7 network, or individual SCTP associations
   are dedicated to each SS7 network context, the Network Appearance
   parameter is not required. In other cases the parameter may be
   configured to be present for the use of the receiver.

   The Network Appearance parameter value is of local significance
   only, coordinated between the SG and AS. Therefore, in the case
   where an AS is connected to more than one SG, the same SS7 network
   context may be identified by different Network Appearance values
   depending over which SG a message is being transmitted/received.

   Where the optional Network Appearance parameter is present, it
   MUST be the first parameter in the message as it defines the
   format of the Protocol Data field.

   IMPLEMENTATION NOTE: For simplicity of configuration it may be
   desirable to use the same NA value across all nodes sharing a

particular network context.

    Routing Context: 32-bits (unsigned integer)

       The Routing Context parameter contains the Routing Context value
       associated with the DATA message.   Where a Routing Key has not
       been coordinated between the SGP and ASP, sending of Routing
       Context is not required. Where multiple Routing Keys and Routing
       Contexts are used across a common association, the Routing Context
       MUST be sent to identify the traffic flow, assisting in the
       internal distribution of Data messages.

    Protocol Data: variable length

       The Protocol Data parameter contains the original SS7 MTP3
       message, including the Service Information Octet and Routing
       Label.

       The Protocol Data parameter contains the following fields:

          Service Indicator,
          Network Indicator,
          Message Priority.

          Destination Point Code,
          Originating Point Code,

          Signalling Link Selection Code (SLS).

          User Protocol Data. Includes:

             MTP3-User protocol elements (e.g., ISUP, SCCP, or TUP
             parameters).

    The Protocol Data parameter is encoded 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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                     Originating Point Code                    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                     Destination Point Code                    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |      SI       |      NI       |      MP       |      SLS      |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                               \
    /                     User Protocol Data                        /
    \                                                               \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

    Originating Point Code: 32 bits (unsigned integer)
    Destination Point Code: 32 bits (unsigned integer)

The Originating and Destination Point Code fields contains the OPC

   and DPC from the routing label of the original SS7 message in Network
   Byte Order, justified to the least significant bit. Unused bits are
   coded `0'.

   Service Indicator: 8 bits (unsigned integer)

   The Service Indicator field contains the SI field from the original
   SS7 message justified to the least significant bit. Unused bits are
   coded `0'.

   Network Indicator: 8-bits (unsigned integer)

   The Network Indicator contains the NI field from the original SS7
   message justified to the least significant bit. Unused bits are
   coded `0'.

   Message Priority: 8 bits (unsigned integer)

   The Message Priority field contains the MP bits (if any) from the
   original SS7 message, both for ANSI-style and TTC-style [29] message
   priority bits. The MP bits are aligned to the least significant bit.
   Unused bits are coded `0'.

   Signalling Link Selection: 8 bits (unsigned integer)

   The Signalling Link Selection field contains the SLS bits from the
   routing label of the original SS7 message justified to the least
   significant bit and in Network Byte Order. Unused bits are coded
   `0'.

   User Protocol Data: (variable length byte string)

   The User Protocol Data field contains a byte string of MTP-User
   information from the original SS7 message starting with the
   first byte of the original SS7 message following the Routing
   Label [7][8][29].

   Correlation Id: 32-bits (unsigned integer)

   The Correlation Id parameter uniquely identifies the MSU carried in
   the Protocol Data within an AS. This Correlation Id parameter is
   assigned by the sending M3UA.

3.4 SS7 Signalling Network Management (SSNM) Messages

3.4.1 Destination Unavailable (DUNA)

   The DUNA message is sent from an SGP in an SG to all concerned ASPs
   to indicate that the SG has determined that one or more SS7

destinations are unreachable. It is also sent by an SGP in response
to a message from the ASP to an unreachable SS7 destination. As an

   implementation option the SG may suppress the sending of subsequent
   "response" DUNA messages regarding a certain unreachable SS7
   destination for a certain period to give the remote side time to
   react. If there is no alternate route via another SG, the MTP3-User
   at the ASP is expected to stop traffic to the affected destination
   via the SG as per the defined MTP3-User procedures.

   The DUNA message contains the following parameters:

      Network Appearance   Conditional
      Routing Context   Conditional
      Affected Point Code   Mandatory
      INFO String   Optional

   The format for DUNA 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Tag = 0x0200           |          Length = 8           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      Network Appearance                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Tag = 0x0006           |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                              \
   /                      Routing Context                         /
   \                                                              \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Tag = 0x0012           |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Mask       |            Affected PC 1                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                              \
   /                            ...                               /
   \                                                              \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Mask       |            Affected PC n                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Tag = 0x0004           |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                              \
   /                         INFO String                          /
   \                                                              \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Network Appearance: 32-bit unsigned integer

The description of Network Appearance in Section 3.3.1 applies
with the exception that Network Appearance does not have to be
the first parameter in this message.

Routing Context: n x 32-bits (unsigned integer)

   The conditional Routing Context parameter contains the Routing
   Context values associated with the DUNA message. Where a Routing
   Key has not been coordinated between the SGP and ASP, sending of

   Routing Context is not required. Where multiple Routing Keys and
   Routing Contexts are used across a common association, the Routing
   Context(s) MUST be sent to identify the concerned traffic flows
   for which the DUNA message applies, assisting in outgoing traffic
   management and internal distribution of MTP-PAUSE indications to
   MTP3-Users at the receiver.

Affected Point Code: n x 32-bits

   The Affected Point Code parameter contains a list of Affected
   Destination 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:

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Mask      |    Network    |    Cluster    |    Member     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

              |MSB----------------------------------------LSB|
```

ITU 14-bit Point Code:

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Mask      |0 0 0 0 0 0 0 0 0 0|Zone |    Region   | SP  |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

                             |MSB-------------------LSB|
```

   It is optional to send an Affected Point Code parameter with more
   than one Affected PC but it is mandatory to receive it. Including
   multiple Affected PCs may be useful when reception of an MTP3
   management message or a linkset event simultaneously affects the
   availability status of a list of destinations at an SG.

Mask: 8-bits (unsigned integer)

The Mask field can be used to identify a contiguous range of
Affected Destination Point Codes. Identifying a contiguous range
of Affected DPCs 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 "wildcarded". For example, a mask of
"8" indicates that the last eight bits of the PC is "wildcarded".
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 "wildcarded". For
a 14-bit ITU Affected PC, this is equivalent to signaling that an
ITU Region is unavailable. A mask value equal (or greater than)
the number of bits in the PC indicates that the entire network
appearance is affected - this is used to indicate network
isolation to the ASP.

INFO String: variable length

The optional INFO String parameter can carry any meaningful UTF-8
[10] character string along with the message. Length of the INFO
String parameter is from 0 to 255 octets. This means that No
procedures are presently identified for its use but the INFO
String MAY be used for debugging purposes. An INFO String with a
zero length parameter is not considered as an error (this means
that the Length field in the TLV will be set to 4).

3.4.2 Destination Available (DAVA)

The DAVA message is sent from an SGP to all concerned ASPs to
indicate that the SG has determined that one or more SS7 destinations
are now reachable (and not restricted), or in response to a DAUD
message if appropriate. If the ASP M3UA layer previously had no
routes to the affected destinations the ASP MTP3-User protocol is
informed and may now resume traffic to the affected destination. The
ASP M3UA layer now routes the MTP3-user traffic through the SG
initiating the DAVA message.

The DAVA message contains the following parameters:

    Network Appearance   Conditional
    Routing Context   Conditional
    Affected Point Code   Mandatory
    INFO String   Optional

The format and description of the Network Appearance, Routing

Context, Affected Point Code and INFO String parameters is the same
as for the DUNA message (See Section 3.4.1).

3.4.3 **Destination State Audit (DAUD)**

   The DAUD message MAY be sent from the ASP to the SGP to audit the
   availability/congestion state of SS7 routes from the SG to one or
   more affected destinations.

   The DAUD message contains the following parameters:

      Network Appearance   Conditional
      Routing Context   Conditional
      Affected Point Code   Mandatory
      INFO String   Optional

   The format and description of DAUD Message parameters is the same as
   for the DUNA message (See Section 3.4.1).

3.4.4 **Signalling Congestion (SCON)**

   The SCON message can be sent from an SGP to all concerned ASPs to
   indicate that an SG has determined that there is congestion in the
   SS7 network to one or more destinations, or to an ASP in response to
   a DATA or DAUD message as appropriate. For some MTP protocol
   variants (e.g., ANSI MTP) the SCON message may be sent when the SS7
   congestion level changes. The SCON message MAY also be sent from the
   M3UA layer of an ASP to an M3UA peer indicating that the congestion
   level of the M3UA layer or the ASP has changed.

   IMPLEMENTATION NOTE: An M3UA node may maintain a timer to control
   congestion notification validity, if desired. This timer will be
   useful in those cases where the peer node fails to indicate
   congestion abatement.

   The SCON message contains the following parameters:

      Network Appearance   Conditional
      Routing Context   Conditional
      Affected Point Code   Mandatory
      Concerned Destination   Optional
      Congestion Indications   Optional
      INFO String   Optional

   The format for SCON 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0200          |           Length = 8          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|                       Network Appearance                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
    |        Tag = 0x0006            |              Length            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                               \
    /                     Routing Context                           /
    \                                                               \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |        Tag = 0x0012            |              Length           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Mask      |               Affected PC 1                    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                               \
    /                          ...                                  /
    \                                                               \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Mask      |               Affected PC n                    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |        Tag = 0x0206           |            Length = 8          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |    reserved   |               Concerned DPC                    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |        Tag = 0x0205           |            Length = 8          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                    Reserved                  | Cong. Level    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |        Tag = 0x0004          |              Length            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                               \
    /                      INFO String                              /
    \                                                               \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format and description of the Network Appearance, Routing
Context, Affected Point Code, and INFO String parameters is the same
as for the DUNA message (See Section 3.4.1).

The Affected Point Code parameter can be used to indicate congestion
of multiple destinations or ranges of destinations.

Concerned Destination: 32-bits

   The optional Concerned Destination parameter is only used if the
   SCON message is sent from an ASP to the SGP. It contains the point
   code of the originator of the message that triggered the SCON
   message. The Concerned Destination parameter contains one
   Concerned Destination Point Code field, a three-octet parameter to
   allow for 14-, 16- and 24-bit binary formatted SS7 Point Codes. A
   Concerned Point Code that is less than 24-bits is padded on the
   left to the 24-bit boundary. Any resulting Transfer Controlled

(TFC) message from the SG is sent to the Concerned Point Code
using the single Affected DPC contained in the SCON message to
populate the (affected) Destination field of the TFC message

Congested Indications: 32-bits

   The optional Congestion Indications parameter contains a
   Congestion Level field. This optional parameter is used to
   communicate congestion levels in national MTP networks with
   multiple congestion thresholds, such as in ANSI MTP3. For MTP
   congestion methods without multiple congestion levels (e.g., the
   ITU international method) the parameter is not included.

Congestion Level field: 8-bits (unsigned integer)

   The Congestion Level field, associated with all of the Affected
   DPC(s) in the Affected Destinations parameter, contains one of the
   following values:

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

   The congestion levels are defined in the congestion method in the
   appropriate national MTP recommendations [7,8].

3.4.5 Destination User Part Unavailable (DUPU)

   The DUPU message is used by an SGP to inform concerned ASPs that a
   remote peer MTP3-User Part (e.g., ISUP or SCCP) at an SS7 node is
   unavailable.

   The DUPU message contains the following parameters:

       Network Appearance   Conditional
       Routing Context   Conditional
       Affected Point Code   Mandatory
       User/Cause   Mandatory
       INFO String   Optional

   The format for DUPU 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0200          |            Length = 8         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     Network Appearance                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0006          |             Length           |
```

```
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     \                                                        \
```

```
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     \                                                        \
```

```
/                        Routing Context                         /
\                                                                \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Tag = 0x0012         |          Length = 8           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Mask = 0    |                 Affected PC                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Tag = 0x0204         |          Length = 8           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Cause             |              User             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Tag = 0x0004         |             Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                                \
/                          INFO String                          /
\                                                                \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

User/Cause: 32-bits

   The Unavailability Cause and MTP3-User Identity fields, associated
   with the Affected PC in the Affected Point Code parameter, are
   encoded as follows:

Unavailability Cause field: 16-bits (unsigned integer)

   The Unavailability Cause parameter provides the reason for the
   unavailability of the MTP3-User. The valid values for the
   Unavailability Cause parameter are shown in the following table.
   The values agree with those provided in the SS7 MTP3 User Part
   Unavailable message. Depending on the MTP3 protocol used in the
   Network Appearance, additional values may be used - the
   specification of the relevant MTP3 protocol variant/version
   recommendation is definitive.

        0   Unknown
        1   Unequipped Remote User
        2   Inaccessible Remote User

   MTP3-User Identity field: 16-bits (unsigned integer)

   The MTP3-User Identity describes the specific MTP3-User that is
   unavailable (e.g., ISUP, SCCP, ...). Some of the valid values for
   the MTP3-User Identity are shown below. The values align with
   those provided in the SS7 MTP3 User Part Unavailable message and
   Service Indicator. Depending on the MTP3 protocol variant/version
   used in the network appearance, additional values may be used.
   The relevant MTP3 protocol variant/version recommendation is

definitive.

        0 to 2   Reserved

```
         3      SCCP
         4      TUP
         5      ISUP
      6 to 8    Reserved
         9      Broadband ISUP
        10      Satellite ISUP
        11      Reserved
        12      AAL type 2 Signalling
        13      Bearer Independent Call Control (BICC)
        14      Gateway Control Protocol
        15      Reserved
```

The format and description of the Affected Point Code parameter is the same as for the DUNA message (See Section 3.4.1.) except that the Mask field is not used and only a single Affected DPC is included. Ranges and lists of Affected DPCs cannot be signaled in a DUPU message, but this is consistent with UPU operation in the SS7 network. The Affected Destinations parameter in an MTP3 User Part Unavailable message (UPU) received by an SGP from the SS7 network contains only one destination.

The format and description of the Network Appearance, Routing Context, and INFO String parameters is the same as for the DUNA message (See Section 3.4.1).

3.4.6 Destination Restricted (DRST)

The DRST message is optionally sent from the SGP to all concerned ASPs to indicate that the SG has determined that one or more SS7 destinations are now restricted from the point of view of the SG, or in response to a DAUD message if appropriate. The M3UA layer at the ASP is expected to send traffic to the affected destination via an alternate SG with route(s) 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 MTP3-User should be informed that traffic to the affected destination can be resumed. In this case, the M3UA 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. It is for use in the "STP" case described in Section 1.4.1.

The DRST message contains the following parameters:

```
   Network Appearance      Conditional
   Routing Context         Conditional
   Affected Point Code     Mandatory
```

INFO String   Optional

    The format and description of the Network Appearance, Routing

Context, Affected Point Code and INFO String parameters is the same
as for the DUNA message (See Section 3.4.1).

3.5 **ASP State Maintenance (ASPSM) Messages**

3.5.1 **ASP Up**

The ASP Up message is used to indicate to a remote M3UA peer that the
adaptation layer is ready to receive any ASPSM/ASPTM messages for all
Routing Keys that the ASP is configured to serve.

The ASP Up message contains the following parameters:

     ASP Identifier   Optional
     INFO String   Optional

The format for ASP Up 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Tag = 0x0011          |            Length = 8         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         ASP Identifier                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Tag = 0x0004          |            Length            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                              \
/                          INFO String                         /
\                                                              \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ASP Identifier: 32-bit unsigned integer

The optional ASP Identifier parameter contains 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 3.8.2).

The format and description of the optional INFO String parameter
is the same as for the DUNA message (See Section 3.4.1).

3.5.2 **ASP Up Acknowledgement (ASP Up Ack)**

The ASP UP Ack message is used to acknowledge an ASP Up message
received from a remote M3UA peer.

The ASP Up Ack message contains the following parameters:
     ASP Identifier   Optional

```
       INFO String                   Optional
```

The format for ASP Up Ack 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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Tag = 0x0011          |          Length = 8           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                        ASP Identifier                         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Tag =0x0004           |            Length             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                               \
    /                          INFO String                          /
    \                                                               \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The optional ASP Identifier parameter is specifically useful for IPSP
communication. In that case the IPSP answering the ASP Up message MAY
include its own ASP Identifier value. For AS-SG communication this
parameter MUST NOT be used.

The format and description of the optional INFO String parameter is
the same as for the DUNA message (See Section 3.4.1). The INFO
String in an ASP Up Ack message is independent from the INFO String
in the ASP Up message (i.e., it does not have to echo back the INFO
String received).

3.5.3 ASP Down

The ASP Down message is used to indicate to a remote M3UA peer that
the adaptation layer is NOT ready to receive DATA, SSNM, RKM or ASPTM
messages.

The ASP Down message contains the following parameters:

    INFO String   Optional

The format for the ASP Down 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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Tag =0x0004           |            Length             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                               \
    /                          INFO String                          /
    \                                                               \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format and description of the optional INFO String parameter is

   the same as for the DUNA message (See Section 3.4.1).

3.5.4 ASP Down Acknowledgement (ASP Down Ack)

   The ASP Down Ack message is used to acknowledge an ASP Down message
   received from a remote M3UA peer.

   The ASP Down Ack message contains the following parameters:

     INFO String   Optional

   The format for the ASP Down Ack 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0004          |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                          INFO String                          /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   The format and description of the optional INFO String parameter is
   the same as for the DUNA message (See Section 3.4.1).

   The INFO String in an ASP Down Ack message is independent from the
   INFO String in the ASP Down message (i.e., it does not have to echo
   back the INFO String received).

3.5.5 Heartbeat (BEAT)

   The BEAT message is optionally used to ensure that the M3UA peers are
   still available to each other. It is recommended for use when the
   M3UA runs over a transport layer other than the SCTP, which has its
   own heartbeat.

   The BEAT message contains the following parameters:

     Heartbeat Data   Optional

   The format for the BEAT message 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0009          |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
```

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

The Heartbeat Data parameter contents are defined by the sending
node. The Heartbeat Data could include, for example, a Heartbeat
Sequence Number and/or Timestamp. The receiver of a BEAT message
does not process this field as it is only of significance to the
sender. The receiver MUST respond with a BEAT Ack message.

3.5.6 Heartbeat Acknowledgement (BEAT Ack)

The BEAT Ack message is sent in response to a received BEAT message.
It includes all the parameters of the received BEAT message, without
any change.

3.6 Routing Key Management (RKM) Messages [Optional]

3.6.1 Registration Request (REG REQ)

The REG REQ message is sent by an ASP to indicate to a remote M3UA
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 REG REQ message contains the following parameters:

    Routing Key   Mandatory

One or more Routing Key parameters MAY be included. The format for
the REG REQ message 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Tag = 0x0207           |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                      Routing Key 1                            /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                           ...                                 /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |        Tag = 0x0207           |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                      Routing Key n                            /
   \                                                               \
```
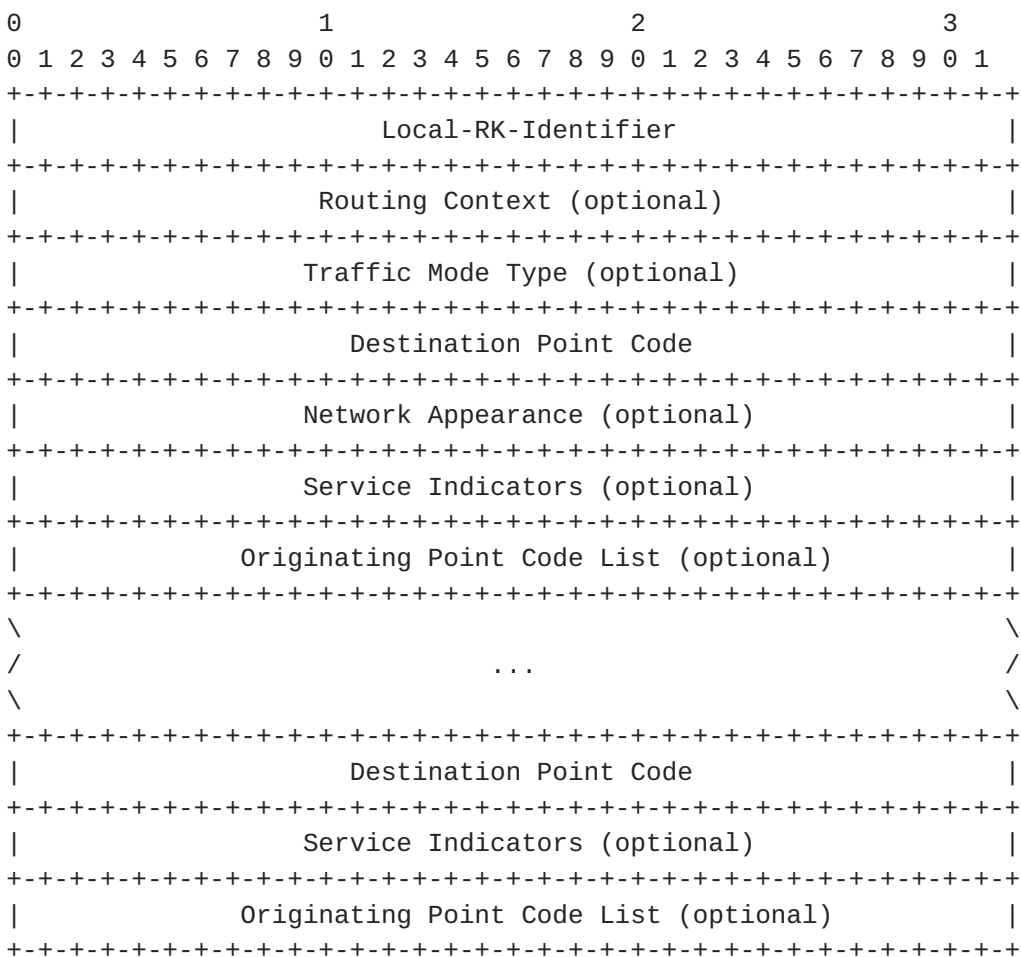
```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Routing Key: variable length

> The Routing Key parameter is mandatory. The sender of this message
> expects that the receiver of this message will create a Routing
> Key entry and assign a unique Routing Context value to it, if the
> Routing Key entry does not already exist.
>
> The Routing Key parameter may be present multiple times in the
> same message. This is used to allow the registration of multiple
> Routing Keys in a single message.

The format of the Routing Key parameter 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Local-RK-Identifier                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Routing Context (optional)                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Traffic Mode Type (optional)                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Point Code                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Network Appearance (optional)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Service Indicators (optional)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Originating Point Code List (optional)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                               \
/                            ...                                /
\                                                               \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Point Code                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Service Indicators (optional)                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|              Originating Point Code List (optional)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

> Note: The Destination Point Code, Service Indicators, and
> Originating Point Code List parameters MAY be repeated as a
> grouping within the Routing Key parameter, in the structure shown
> above.

Local-RK-Identifier: 32-bit unsigned integer

The mandatory Local-RK-Identifier field is used to uniquely
identify the registration request. The Identifier value is
assigned by the ASP, and is used to correlate the response in an

REG RSP message with the original registration request. The
Identifier value must remain unique until the REG RSP message is
received.

The format of the Local-RK-Identifier field 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Tag = 0x020a          |          Length = 8           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Local-RK-Identifier value                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Traffic Mode Type: 32-bit (unsigned integer)

The optional Traffic Mode Type parameter identifies the traffic mode
of operation of the ASP(s) within an Application Server. The format
of the Traffic Mode Type Identifier 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Tag = 0x000b          |          Length = 8           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        Traffic Mode Type                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The valid values for Traffic Mode Type are shown in the following
table:

```
     1     Override
     2     Loadshare
     3     Broadcast
```

Destination Point Code:

The Destination Point Code parameter is mandatory, and
Identifies the Destination Point Code of incoming SS7 traffic
for which the ASP is registering. For an alias point code
configuration, the DPC parameter would be repeated for each
point code. The format is the same as described for the
Affected Destination parameter in the DUNA message (See Section
3.4.1). Its format is:

```
 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 = 0x020b          |          Length = 8           |
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Mask = 0    |                Destination Point Code         |
```

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

Network Appearance:

   The optional Network Appearance parameter field identifies the SS7
   network context for the Routing Key, and has the same format as in
   the DATA message (See Section 3.3.1) with the exception that it
   does not have to be the first parameter in the message. The
   absence of the Network Appearance parameter in the Routing Key
   indicates the use of any Network Appearance value. Its format is:

```
    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 = 0x0200          |         Length = 8            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Network Appearance                      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Service Indicators (SI): n X 8-bit integers

   The optional SI [7,8] field contains one or more Service
   Indicators from the values as described in the MTP3-User Identity
   field of the DUPU message. The absence of the SI parameter in the
   Routing Key indicates the use of any SI value, excluding of course
   MTP management. Where an SI parameter does not contain a multiple
   of four SIs, the parameter is padded out to 32-byte alignment.

   The SI format is:

```
    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 = 0x020c          |             Length           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     SI #1     |     SI #2     |     SI #3     |    SI #4      |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   /                              ...                              /
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     SI #n     |             0 Padding, if necessary           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

OPC List:

   The Originating Point Code List parameter contains one or more SS7
   OPC entries, and its format is the same as the Destination Point
   Code parameter. The absence of the OPC List parameter in the
   Routing Key indicates the use of any OPC value,

```
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                   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 = 0x020e          |              Length           |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |   Mask = 0   |           Origination Point Code #1          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |   Mask = 0   |           Origination Point Code #2          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     /                             ...                             /
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |   Mask = 0   |           Origination Point Code #n          |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

[3.6.2](#) **Registration Response (REG RSP)**

The REG RSP message is used as a response to the REG REQ message from
a remote M3UA peer. 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 M3UA
Traffic Management protocol.

The REG RSP message contains the following parameters:

Registration Result   Mandatory

One or more Registration Result parameters MUST be included. The
format for the REG RSP message 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
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |        Tag = 0x0208         |              Length            |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                    Registration Result 1                     |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     \                                                              \
     /                             ...                              /
     \                                                              \
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |        Tag = 0x0208         |              Length            |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                    Registration Result n                     |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Registration Results:

   The Registration Result parameter contains the registration result
   for a single Routing Key in an REG REQ message. The number of
   results in a single REG RSP message MUST be anywhere from one to
   the total number of number of Routing Key parameters found in the

corresponding REG REQ message. Where multiple REG RSP messages
are used in reply to REG REQ message, a specific result SHOULD be

in only one REG RSP message. The format of each result 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Tag = 0x020a        |          Length = 8           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Local-RK-Identifier value                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Tag = 0x0212        |          Length = 8           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     Registration Status                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Tag = 0x0006        |          Length = 8           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Routing Context                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Local-RK-Identifier: 32-bit integer

   The Local-RK-Identifier contains the same value as found in the
   matching Routing Key parameter found in the REG REQ message (See
   Section 3.6.1).

Registration Status: 32-bit integer

   The Registration Result 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 DPC
     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 Handling Mode
     11   Error - Routing Key Change Refused
     12   Error - Routing Key Already Registered

Routing Context: 32-bit integer

   The Routing Context field contains the Routing Context value for

the associated Routing Key if the registration was successful. It
is set to "0" if the registration was not successful.

3.6.3 **Deregistration Request (DEREG REQ)**

   The DEREG REQ message is sent by an ASP to indicate to a remote M3UA
   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 DEREG REQ message contains the following parameters:

      Routing Context   Mandatory

   The format for the DEREG REQ message 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0006          |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                      Routing Context                          /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Routing Context: n X 32-bit integers

      The Routing Context parameter contains (a list of) integers
      indexing the Application Server traffic that the sending ASP is
      currently registered to receive from the SGP but now wishes to
      deregister.

3.6.4 **Deregistration Response (DEREG RSP)**

   The DEREG RSP message is used as a response to the DEREG REQ message
   from a remote M3UA peer.

   The DEREG RSP message contains the following parameters:

      Deregistration Result   Mandatory

   One or more Deregistration Result parameters MUST be included. The
   format for the DEREG RSP message 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0209          |             Length            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Deregistration Result 1                    |
```

```
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       \                                                      \
```

```
     /                              ...                              /
     \                                                               \
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |           Tag = 0x0209        |            Length            |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                   Deregistration Result n                   |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Deregistration Results:

   The Deregistration Result parameter contains the deregistration
   status for a single Routing Context in a DEREG REQ message. The
   number of results in a single DEREG RSP message MAY be anywhere
   from one to the total number of number of Routing Context values
   found in the corresponding DEREG REQ message.

   Where multiple DEREG RSP messages are used in reply to DEREG REQ
   message, a specific result SHOULD be in only one DEREG RSP
   message. The format of each result 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |           Tag = 0x0006        |            Length = 8         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                        Routing Context                        |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |           Tag = 0x0213        |            Length = 8         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                     Deregistration Status                     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Routing Context: 32-bit integer

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

   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
```

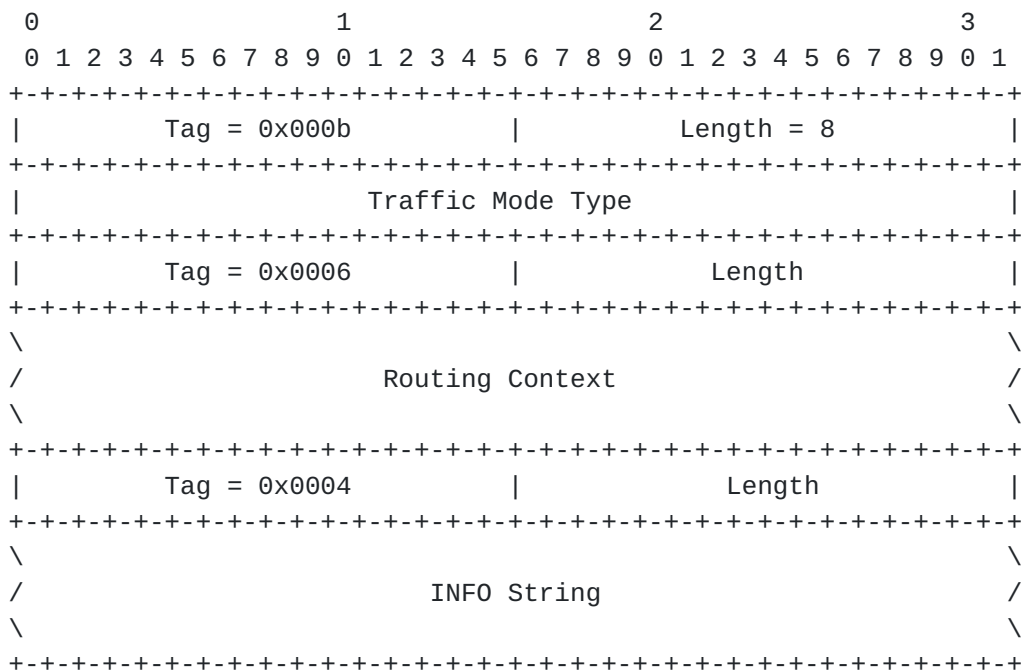**3.7** **ASP Traffic Maintenance (ASPTM) Messages**

3.7.1 **ASP Active**

   The ASP Active message is sent by an ASP to indicate to a remote M3UA
   peer that it is ready to process signalling traffic for a particular
   Application Server. The ASP Active message affects only the ASP
   state for the Routing Keys identified by the Routing Contexts, if
   present.

   The ASP Active message contains the following parameters:

      Traffic Mode Type   Optional
      Routing Context   Optional
      INFO String   Optional

   The format for the ASP Active message 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x000b          |          Length = 8           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Traffic Mode Type                       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0006          |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                       Routing Context                         /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0004          |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                         INFO String                           /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

   Traffic Mode Type: 32-bit (unsigned integer)

      The Traffic Mode Type parameter identifies the traffic mode of
      operation of the ASP within an AS. The valid values for Traffic
      Mode Type are shown in the following table:

         1   Override
         2   Loadshare
         3   Broadcast

Within a particular Routing Context, Override, Loadshare and
Broadcast SHOULD NOT be mixed. The Override value indicates that

the ASP is operating in Override mode, and the ASP takes over all
traffic in an Application Server (i.e., primary/backup operation),
overriding any currently active ASPs in the AS. In Loadshare
mode, the ASP will share in the traffic distribution with any
other currently active ASPs. In Broadcast mode, the ASP will
receive the same messages as any other currently active ASP.

Routing Context: n X 32-bit integers

The optional Routing Context parameter contains (a list of)
integers indexing the Application Server traffic that the sending
ASP is configured/registered to receive.

There is one-to-one relationship between an index entry and an SGP
Routing Key or AS Name. Because an AS can only appear in one
Network Appearance, the Network Appearance parameter is not
required in the ASP Active 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
signalling traffic that the ASP is currently configured to receive
from the SGP. For example, an ASP could be configured to support
call processing for multiple ranges of PSTN trunks and therefore
receive related signalling traffic, identified by separate SS7
DPC/OPC/SI ranges.

The format and description of the optional INFO String parameter is
the same as for the DUNA message (See Section 3.4.1).

3.7.2 ASP Active Acknowledgement (ASP Active Ack)

The ASP Active Ack message is used to acknowledge an ASP Active
message received from a remote M3UA peer.

The ASP Active Ack message contains the following parameters:

```
Traffic Mode Type      Optional
Routing Context        Optional
INFO String            Optional
```

The format for the ASP Active Ack message 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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |           Tag = 0x000b         |           Length = 8          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                       Traffic Mode Type                       |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |           Tag = 0x0006         |             Length            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                               \
    /                       Routing Context                         /
    \                                                               \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |           Tag = 0x0004         |             Length            |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                               \
    /                         INFO String                           /
    \                                                               \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format and description of the optional INFO String parameter is
the same as for the DUNA message (See Section 3.4.1).

The INFO String in an ASP Active Ack message is independent from the
INFO String in the ASP Active message (i.e., it does not have to echo
back the INFO String received).

The format of the Traffic Mode Type and Routing Context parameters is
the same as for the ASP Active message. (See Section 3.7.1).

3.7.3 ASP Inactive

The ASP Inactive message is sent by an ASP to indicate to a remote
M3UA peer that it is no longer an active ASP to be used from within a
list of ASPs. The ASP Inactive message affects only the ASP state in
the Routing Keys identified by the Routing Contexts, if present.

The ASP Inactive message contains the following parameters:
    Routing Context   Optional
    INFO String   Optional

The format for the ASP Inactive 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
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Tag = 0x0006           |             Length             |
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                              \
/                     Routing Context                         /
\                                                              \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Tag = 0x0004          |            Length           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                              \
/                       INFO String                           /
\                                                              \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format and description of the optional Routing Context and INFO
String parameters is the same as for the ASP Active message (See
Section 3.5.5.)

3.7.4 ASP Inactive Acknowledgement (ASP Inactive Ack)

The ASP Inactive Ack message is used to acknowledge an ASP Inactive
message received from a remote M3UA peer.

The ASP Inactive Ack message contains the following parameters:

      Routing Context   Optional
      INFO String   Optional

The format for the ASP Inactive Ack message 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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          Tag = 0x0006          |            Length           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                              \
    /                     Routing Context                         /
    \                                                              \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          Tag = 0x0004          |            Length           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    \                                                              \
    /                       INFO String                           /
    \                                                              \
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The format and description of the optional INFO String parameter is
the same as for the DUNA message (See Section 3.4.1.)

The INFO String in an ASP Inactive Ack message is independent from
the INFO String in the ASP Inactive message (i.e., it does not have

to echo back the INFO String received).

The format of the Routing Context parameter is the same as for the
ASP Inactive message. (See Section 3.7.3).

3.8 Management (MGMT) Messages
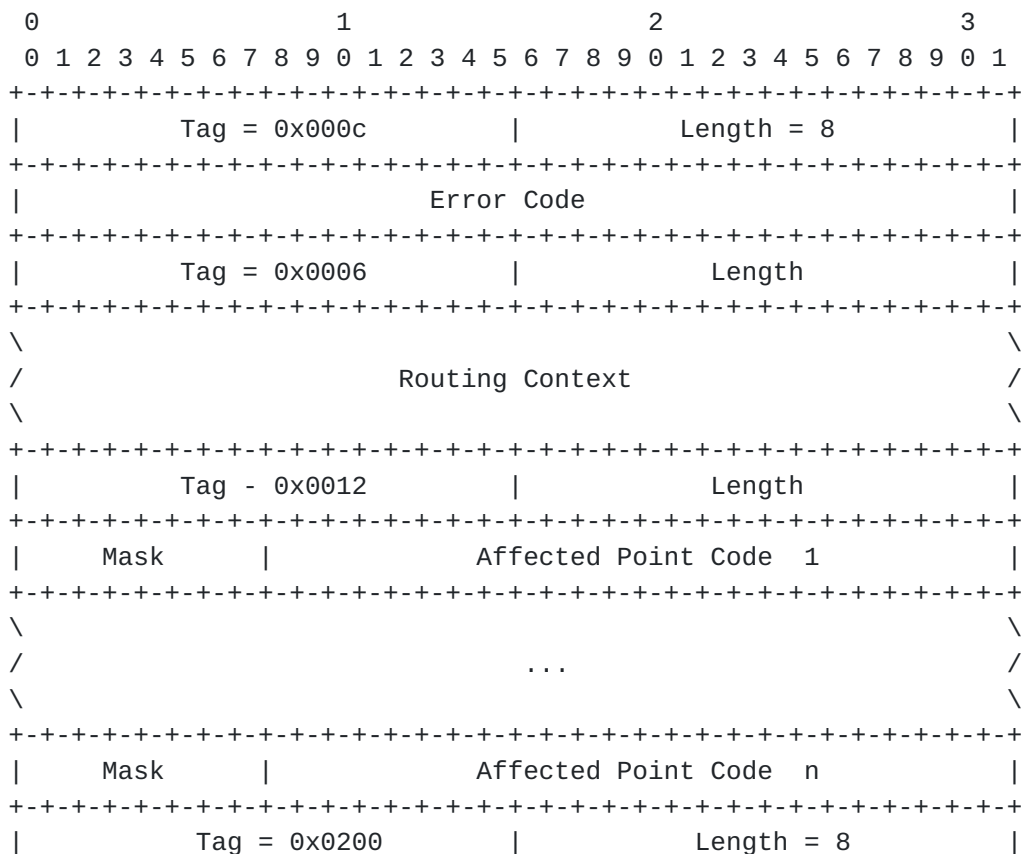
3.8.1 Error

The Error message is used to notify a peer of an error event
associated with an incoming message. For example, the message type
might be unexpected given the current state, or a parameter value
might be invalid. Error messages MUST NOT be generated in response to
other Error messages.

The Error message contains the following parameters:

```
    Error Code                Mandatory
    Routing Context           Mandatory*
    Network Appearance        Mandatory*
    Affected Point Code       Mandatory*
    Diagnostic Information     Conditional

    (*) Only mandatory for specific Error Codes
```

The format for the Error message 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x000c          |          Length = 8           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Error Code                           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag = 0x0006          |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                       Routing Context                         /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |         Tag - 0x0012          |            Length             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Mask      |         Affected Point Code  1                |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   \                                                               \
   /                            ...                                /
   \                                                               \
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Mask      |         Affected Point Code  n                |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |          Tag = 0x0200         |           Length = 8          |
```

```
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                    Network Appearance                   |
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Tag = 0x0007          |             Length           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                                \
/                    Diagnostic Information                      /
\                                                                \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Error Code: 32-bits (unsigned integer)

   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 M3UA
   0x03   Unsupported Message Class
   0x04   Unsupported Message Type
   0x05   Unsupported Traffic Mode Type
   0x06   Unexpected Message

   0x07   Protocol Error
   0x08   Not used in M3UA
   0x09   Invalid Stream Identifier
   0x0a   Not used in M3UA
   0x0b   Not used in M3UA
   0x0c   Not used in M3UA
   0x0d   Refused - Management Blocking
   0x0e   ASP Identifier Required
   0x0f   Invalid ASP Identifier
   0x10   Not Used in M3UA
   0x11   Invalid Parameter Value
   0x12   Parameter Field Error
   0x13   Unexpected Parameter
   0x14   Destination Status Unknown
   0x15   Invalid Network Appearance
   0x16   Missing Parameter
   0x17   Not Used in M3UA
   0x18   Not Used in M3UA
   0x19   Invalid Routing Context
   0x1a   No Configured AS for ASP

   The "Invalid Version" error is sent if a 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.

   The "Unsupported Message Class" error is sent if a message with an

unexpected or unsupported Message Class is received. For this error,
the Diagnostic Information parameter MUST be included with the first
40 bytes of the offending message.

The "Unsupported Message Type" error is sent if a message with an
unexpected or unsupported Message Type is received. For this error,
the Diagnostic Information parameter MUST be included with the first
40 bytes of the offending message.

The "Unsupported Traffic Mode Type" 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 (e.g., a Management message was
received on a stream other than "0").

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 which 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 sent by an 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 is sent if a message, other than ASP-Active, is received from a peer with an invalid Routing Context value. The invalid Routing Context(s) MUST be included in the Error message.

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. This error is also sent when an ASP-Active message is received with an unconfigured RC and the invalid Routing Context(s) MUST be then included in the Error message.

Diagnostic Information: variable length

   When included, the optional Diagnostic information can be any information germane to the error condition, to assist in identification of the error condition. The Diagnostic information SHOULD contain the offending message. The Diagnostic Information parameter with a zero length parameter is not considered as an error (this means that the Length field in the TLV will be set to 4).

3.8.2 Notify

The Notify message used to provide an autonomous indication of M3UA events to an M3UA peer.

The Notify message contains the following parameters:

```
   Status                      Mandatory
   ASP Identifier              Optional
```

```
    Routing Context          Optional
    INFO String              Optional
```

The format for the Notify message 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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          Tag = 0x000d         |           Length = 8          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          Status Type          |       Status Information       |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          Tag = 0x0011         |           Length = 8          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                         ASP Identifier                        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          Tag = 0x0006         |             Length            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 \                                                               \
 /                        Routing Context                        /
 \                                                               \
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          Tag = 0x0004         |             Length            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 \                                                               \
 /                          INFO String                          /
 \                                                               \
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Status Type: 16-bits (unsigned integer)

   The Status Type parameter identifies the type of the Notify
   message. The following are the valid Status Type values:

      1   Application Server State Change (AS-State_Change)
      2   Other

Status Information: 16-bits (unsigned integer)

   The Status Information parameter contains more detailed
   information for the notification, based on the value of the Status
   Type. If the Status Type is AS-State_Change the following Status
   Information values are used:

      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
     ASP_INACTIVE ASP in the AS that another ASP is required to handle
     the load of the AS (Loadsharing or Broadcast mode).

   - For the Alternate ASP Active case, an ASP is informed when an
     alternate ASP transitions to the ASP-ACTIVE state in Override mode.
     The ASP Identifier (if available) of the Alternate ASP MUST be
     placed in the message.

   - For the ASP Failure case, the SGP is indicating to ASP(s) in the AS
     that one of the ASPs has failed. The ASP Identifier (if available)
     of the failed ASP MUST be placed in the message.

   The format and description of the optional ASP Identifier is the same
   as for the ASP Up message (See Section 3.5.1). The format and
   description of the Routing Context and Info String parameters is the
   same as for the ASP Active message (See Section 3.7.1)

4. Procedures

   The M3UA layer needs to respond to various local primitives it
   receives from other layers as well as the messages that it receives
   from the peer M3UA layer. This section describes the M3UA procedures
   in response to these events.

4.1 Procedures to Support the M3UA-User

4.1.1 Receipt of Primitives from the M3UA-User

   On receiving an MTP-TRANSFER request primitive from an upper layer at
   an ASP/IPSP, or the nodal interworking function at an SGP, the M3UA
   layer sends a corresponding DATA message (see Section 3) to its M3UA
   peer. The M3UA peer receiving the DATA message sends an MTP-TRANSFER
   indication primitive to the upper layer.

   The M3UA message distribution function (see Section 1.4.2.1)
   determines the Application Server (AS) based on comparing the
   information in the MTP-TRANSFER 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 loadshared 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 or ISUP CIC. 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 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 M3UA 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 M3UA layer will attempt to establish an SCTP association with the remote M3UA 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 M3UA layer. At the SGP or IPSP that initiated the request, the M3UA layer will send an M-SCTP_ESTABLISH confirm primitive to Layer Management when the association setup is complete. At the peer M3UA

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 initiates the teardown of an SCTP association. The M3UA 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 M3UA layer. At the M3UA Layer
that initiated the request, the M3UA layer will send an M-
SCTP_RELEASE confirm primitive to Layer Management when the
association shutdown is complete. At the peer M3UA 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 M3UA layer
simply maps the M-SCTP_STATUS request primitive to an SCTP-STATUS
primitive to the SCTP layer. When the SCTP responds, the M3UA layer
maps the association status information to an M-SCTP_STATUS confirm
primitive. No peer protocol is invoked.

Similar LM-to-M3UA-to-SCTP and/or SCTP-to-M3UA-to-LM primitive
mappings can be described for the various other SCTP Upper Layer
primitives in RFC2960 [17] 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 M3UA Notify or Error message respectively. These
indications can also be generated based on local M3UA events.

An M-ASP_STATUS request primitive supports a Layer Management query
of the status of a particular local or remote ASP. The M3UA layer
responds with the status in an M-ASP_STATUS confirm primitive. No
M3UA peer protocol is invoked.

An M-AS_STATUS request supports a Layer Management query of the
status of a particular AS. The M3UA responds with an M-AS_STATUS
confirm primitive. No M3UA 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 M3UA 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 M3UA

peer at an SGP or IPSP.

4.2.1 **Receipt of M3UA Peer Management Messages**

Upon successful state changes resulting from reception of ASP Up, ASP
Down, ASP Active and ASP Inactive messages from a peer M3UA, the M3UA
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 M3UA Notify or Error message. These indications can also be
generated based on local M3UA events.

All non-Transfer and non-SSNM, messages, except BEAT and BEAT Ack,
SHOULD be sent with sequenced delivery to ensure ordering. ASPTM
messages MAY be sent on one of the streams used to carry the 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 M3UA 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 M3UA message distribution function.
Similarly, where IPSPs use M3UA in a point-to-point fashion, the M3UA
layer in an IPSP maintains the state of remote IPSPs.

Two IPSP models are defined with regards to the number of messages
that are needed to a IPSP state change. They are defined as follows:

1- IPSP Single Exchange (SE) model. Only a single exchange of ASPTM
   or ASPSM messages is needed to change the IPSP state. This means
   that a set of request from one end and acknowledge from the other
   will be enough. This configuration requires static RK
   configuration.

2- IPSP Double Exchange (DE) model. Both IPSPs have to send request
   messages and both IPSPs have to acknowledge the request messages
   from the other end. This results in a double exchange of ASPTM and
   ASPSM message, one from each end. This configuration supports
   dynamic routing key configuration by using RKM messages in the
   same way as ASP-SGP scenario.

In order to ensure interoperability, an M3UA implementation
supporting IPSP communication MUST support IPSP SE model and MAY
implement IPSP DE model.

In section 4.3.1: ASP/IPSP States, only the SGP-ASP and the IPSP SE

scenarios are described. For the IPSP DE model, both IPSPs MUST
follow the SGP side of the SGP-ASP procedures.

In section 4.3.2, only the SGP-ASP scenario is described. All of the
procedures referring to an AS served by ASPs are also applicable to
ASes served by IPSPs.

In section 4.3.3, only the Management procedures for the SGP-ASP
scenario are described. The corresponding Management procedures for
IPSPs are directly inferred.

The remaining sections contain specific IPSP Considerations sub-
sections.

4.3.1 ASP States

The state of each remote ASP/IPSP, in each AS that it is configured
to operate, is maintained in the peer M3UA layer (i.e. in the SGP or
peer IPSP, respectively). The state of a particular ASP/IPSP in a
particular AS changes due to events. The events include:

* Reception of messages from the peer M3UA layer at the ASP/IPSP;
* Reception of some messages from the peer M3UA layer at other
  ASPs/IPSPs in the AS (e.g., ASP Active message indicating
  "Override");
* Reception of indications from the SCTP layer; or
* Local Management intervention.

The ASP/IPSP state transition diagram is shown in Figure 3. The
possible states of an ASP/IPSP are:

ASP-DOWN: The remote M3UA peer at the ASP/IPSP is unavailable and/or
the related SCTP association is down. Initially all ASPs/IPSPs will
be in this state. An ASP/IPSP in this state SHOULD NOT be sent any
M3UA messages, with the exception of Heartbeat, ASP Down Ack and
Error messages.

ASP-INACTIVE: The remote M3UA peer at the ASP/IPSP is available (and
the related SCTP association is up) but application traffic is
stopped. In this state the ASP/IPSP SHOULD NOT be sent any DATA or
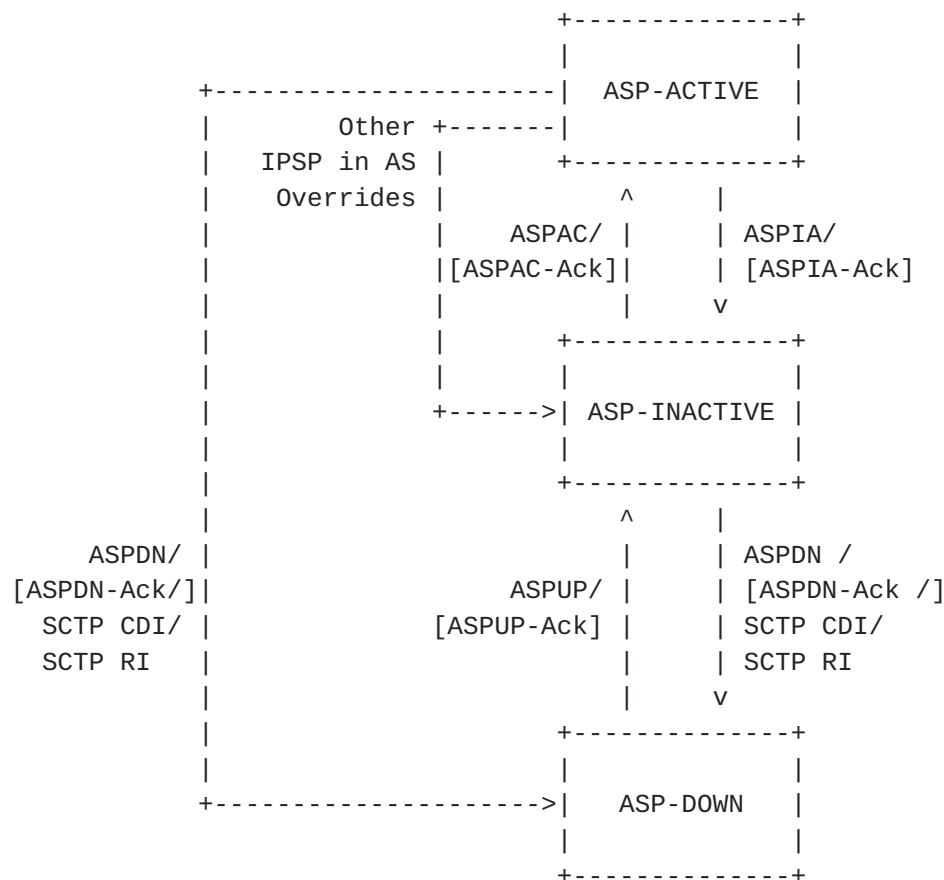SSNM messages for the AS for which the ASP/IPSP is inactive.

ASP-ACTIVE: The remote M3UA peer at the ASP/IPSP is available and
application traffic is active (for a particular Routing Context or
set of Routing Contexts).

SCTP CDI: The SCTP CDI denotes the local SCTP layer's Communication
Down Indication to the Upper Layer Protocol (M3UA) 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 (M3UA) on an SG. The local SCTP will send this indication
   when it detects a restart from the ASP's/IPSP's peer SCTP layer.

             Figure 3: ASP State Transition Diagram, per AS


```
                               +--------------+
                               |              |
               +---------------------|  ASP-ACTIVE  |
               |         Other +-------|              |
               |       IPSP in AS |       +--------------+
               |        Overrides |            ^      |
               |                  |   ASPAC/ |      | ASPIA/
               |                  |[ASPAC-Ack]|      | [ASPIA-Ack]
               |                  |           |      v
               |                  |       +--------------+
               |                  |       |              |
               |              +------>|  ASP-INACTIVE |
               |                  |       |              |
               |                  |       +--------------+
               |                  |            ^      |
        ASPDN/ |                  |            |      | ASPDN /
     [ASPDN-Ack/]|                |    ASPUP/ |      | [ASPDN-Ack /]
       SCTP CDI/ |                | [ASPUP-Ack] |      | SCTP CDI/
       SCTP RI   |                |            |      | SCTP RI
                 |                |            |      v
                 |                |       +--------------+
                 |                |       |              |
         +---------------------->|   ASP-DOWN   |
                 |                |       |              |
                 |                |       +--------------+
```

   The transitions in brackets are just valid for the IPSP SE model
   communication while the rest are valid for both ASPs and IPSPs.

[4.3.2](#) **AS States**

   The state of the AS is maintained in the M3UA layer on the SGPs. 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 the ASPs are in ASP-DOWN state. Initially the AS will be in
   this state. An Application Server is in the AS-DOWN state when it is
   removed from a configuration.

   AS-INACTIVE: The Application Server is available but no application
   traffic is active. One or more ASPs are in ASP-INACTIVE state and/or
   the number of ASPs in ASP-ACTIVE state has not reached n. The
   recovery timer T(r) is not running or has expired.
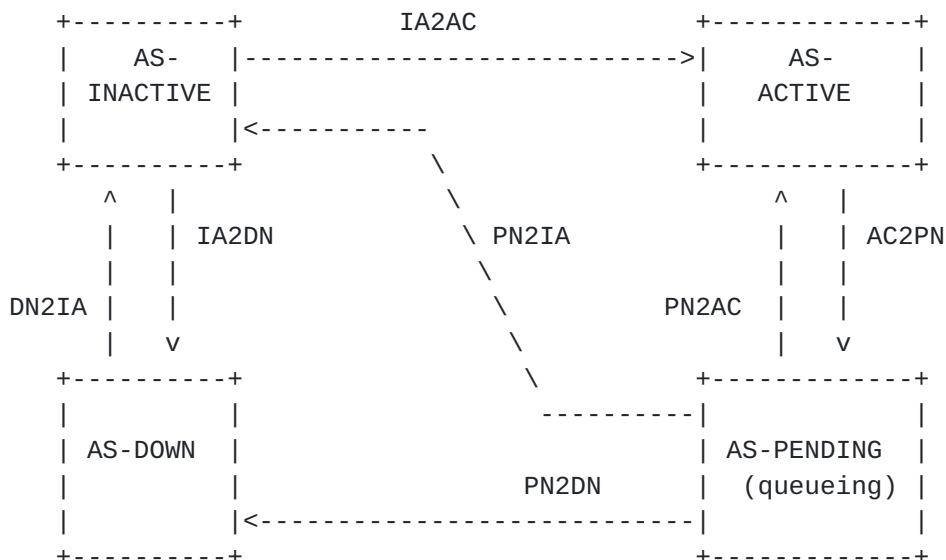
   AS-ACTIVE: The Application Server is available and application
   traffic is active. The AS moves to this state after being in AS-
   INACTIVE and getting n ASPs in ASP-ACTIVE state or, after reaching
   AS-ACTIVE and keeping one or more ASPs in ASP-ACTIVE state.
   When it is considered that one ASP is enough to handle traffic
   (smooth start), the AS in AS-INACTIVE MAY reach the AS-ACTIVE as soon
   as the first ASP moves to the ASP-ACTIVE state.

   AS-PENDING: The last active ASP has transitioned from ASP-ACTIVE to
   ASP-INACTIVE or ASP-DOWN. 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, the SGP MAY stop
   queuing messages and discards all
   previously queued messages. The AS will move to the AS-INACTIVE state
   if at least the number of ASPs in ASP-INACTIVE sum n, 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 preconfigured and an n+k redundancy model.

                   Figure 5: AS State Transition Diagram

        +----------+   IA2AC   +-------------+
        | AS- |---------------------------->| AS- |
        | INACTIVE | | ACTIVE |
        | |<---------- | |
        +----------+   \   +-------------+
           ^ | \   ^ |
           | | IA2DN   \ PN2IA | | AC2PN
           | | \ | |
      DN2IA | | \   PN2AC | |
           | v   \ | v
        +----------+   \   +-------------+
        | | ----------| | |
        | AS-DOWN | | | AS-PENDING |
        | | PN2DN | | (queueing) |
        | |<----------------------------| |
        +----------+   +-------------+

DN2IA: One ASP moves from ASP-DOWN to ASP-INACTIVE state.

IA2DN: The last ASP in ASP-INACTIVE moves to ASP-DOWN causing that the all the ASPs are in ASP-DOWN state.

IA2AC: one ASP moves to ASP-ACTIVE, causing number of ASPs in the ASP-ACTIVE state to be n.
In a special case of smooth start, this transition MAY be done when the first ASP moves to ASP-ACTIVE state.

AC2PN: the last ASP in ASP-ACTIVE state moves to ASP-INACTIVE or ASP-DOWN states, causing the number of ASPs in ASP-ACTIVE drop below 1.

PN2AC: One ASP moves to ASP-ACTIVE.

PN2IA: T(r) Expiry, n or more ASPs are in ASP-INACTIVE.

PN2DN: T(r) Expiry, all the ASPs are in ASP-DOWN state.

An AS becomes AS-ACTIVE right after n ASPs reach the ASP-ACTIVE state during the start-up phase (except for smooth start). Once the traffic is flowing, an AS keeps the AS-ACTIVE state till the last ASP turns to another state different to ASP-ACTIVE, avoiding unnecessary traffic disturbances as long as there are ASPs available, in the assumption that the system will not always be exposed to the maximum load.

There are other cases where the AS/ASP configuration data is created dynamically. In those cases 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 nth successful REG REQ from an ASP belonging to that AS. Another example is where the AS/ASP configuration data is not created until the nth ASP successfully enters the ASP-ACTIVE state. In this latter case the AS-ACTIVE state is entered directly.

4.3.3 M3UA 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) and assuming that the local M3UA-User is ready, the local M3UA 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 M3UA 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.
At an ASP, the MTP3-User will be informed of the unavailability of
any affected SS7 destinations through the use of MTP-PAUSE indication
primitives.

In the case of SCTP-COMMUNICATION_DOWN, the SCTP client MAY try to
re-establish the SCTP Association. This MAY be done by the M3UA
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 M3UA 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 M3UA 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 M3UA 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 lockout) 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
M3UA messages (e.g., ASP Active or REG REQ). If the SGP receives any
other M3UA messages before an ASP Up message is received (other than
ASP Down - see Section 4.3.4.2), the SGP MAY 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). In addition, the remote ASP
state is changed to ASP-INACTIVE in all relevant Application Servers
and all registered Routing Keys are considered deregistered.

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 M3UA Version Control and ASP Up

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. See
section 4.8 for more on this issue.

4.3.4.1.2 IPSP Considerations (ASP Up)

An IPSP may be considered in the ASP-INACTIVE state after an ASP Up
or ASP Up Ack has been received from it. An IPSP can be considered
in the ASP-DOWN state after an ASP Down or ASP Down 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, when using IPSP DE model, an interchange of ASP Up
messages from each end MUST be performed. Four messages are needed
for completion.

If for any local reason (e.g., management lockout) an 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 M3UA
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 M3UA

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 and move the ASP to
the ASP-ACTIVE state in all Application Servers.

For the Application Servers that the ASP can be successfully
activated, 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 value 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 or SSNM 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 ASP Active message will be responded in the following way as a
function of the presence/need of the RC parameter:

- If the RC parameter is included in the ASP Active message and the
  corresponding RK has been previously defined (by either static
  configuration or dynamic registration), the peer node MUST respond
  with an ASP Active Ack message if it is ready to handle traffic;
  otherwise it will not respond (meaning that it is not ready to
  become active). This is valid for either: ASP was in ASP-ACTIVE or
  ASP-INACTIVE states.

- If the RC parameter is included in the ASP Active message and a
  corresponding RK has not been previously defined (by either static

configuration or dynamic registration), the peer MUST respond with
an ERROR message with Error Code = "No configured AS for ASP".

- If the RC parameter is not included in the ASP Active message,
  there are RKs defined (by either static configuration or dynamic
  registration) and RC is not mandatory, the peer node SHOULD respond
  with an ASP Active Ack message and activate all the RKs it has
  defined for that specific ASP.

- If the RC parameter is not included in the ASP Active message,
  there are RKs defined (by either static configuration or dynamic
  registration) and RC is mandatory, the peer node MUST respond with
  and ERROR message with the Error Code = "Missing Parameter".

- If the RC parameter is not included in the ASP Active message,
  there are RKs defined (by either static configuration or dynamic
  registration) and RC is not mandatory, the peer node MUST respond
  with an ASP Active Ack message if it is ready to handle traffic;
  otherwise it will not respond (meaning that it is not ready to
  become active).

- If the RC parameter is not included in the ASP Active message and
  there are no RKs defined, the peer node SHOULD respond with and
  ERROR message with the Error Code = "No configured AS for ASP".

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 M3UA layer: Override, Loadshare 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
loadsharing 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, SCCP SSN, ISUP CIC value).
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). In this case, the SGP or IPSP SHOULD withhold
the Notify (AS-ACTIVE) until there are sufficient resources.

For the n+k redundancy case, ASPs which are in that AS should
coordinate among themselves the number of active ASPs in the AS, and
should start sending traffic only after n ASPs are active.
All ASPs within a loadsharing mode AS must be able to process any
Data message received for the AS, to accommodate any potential
failover 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.

At start-up or re-start phases, an SGP or IPSP, upon reception of an
ASP Active message for the first ASP in a Loadshare AS, SHOULD NOT
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). In this case, the

SGP or IPSP SHOULD withhold the Notify (AS-ACTIVE) until there are
sufficient resources.

For the n+k redundancy case, ASPs which are in that AS should
coordinate among themselves the number of active ASPs in the AS, and
should start sending traffic only after n ASPs are active.

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

4.3.4.3.1 IPSP Considerations (ASP Active)

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, when using IPSP DE model, an interchange of ASP Active
messages from each end MUST be performed. Four messages are needed
for completion.

4.3.4.4 ASP Inactive Procedures

When an ASP wishes to withdraw from receiving traffic within an AS,
or the ASP wants to initiate the process of deactivation, the ASP
sends an ASP Inactive message to the SGP or IPSP.

An ASP Inactive message MUST always be responded by the peer
(although other messages may be sent in the middle) in the following
way:

   - If the ASP Inactive message contains a RC parameter and the
      corresponding RK is defined (by either static configuration or
      dynamic registration), the peer MUST respond with an ASP
      Inactive Ack message.

   - If the ASP Inactive message contains a RC parameter that is not
      defined (by either static configuration or dynamic
      registration), the peer MUST respond with an ERROR message with
      Error Code = "Invalid Routing Context".

   - If the ASP Inactive message does not contain a RC parameter and
      the RK is defined (by either static configuration or dynamic

registration), the peer must turn the ASP/IPSP to ASP-INACTIVE

state in all the ASes it serves and MUST respond with an ASP
Inactive Ack message.

- If the ASP Inactive message does not contain a RC parameter and
  the RK is not defined (by either static configuration or dynamic
  registration), the peer MUST respond with an ERROR message with
  Error Code = "No configured AS for ASP".

The action of sending the ASP Inactive message MAY be initiated at
the ASP by an M-ASP_INACTIVE request primitive from Layer Management
or MAY be initiated automatically by an M3UA 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 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 Loadshare mode AS, the SGP moves the ASP to the
ASP-INACTIVE state and the AS traffic is reallocated across the
remaining ASPs in the state ASP-ACTIVE, as per the loadsharing
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 (ASP Inactive)

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, when using IPSP DE model, an interchange of ASP
Inactive messages from each end MUST be performed. Four messages are
needed 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, with
appropriate 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 related
acknowledgement messages (e.g., ASP Up Ack, ASP Down Ack, ASP Active
Ack, or ASP Inactive Ack).

When an ASP moves from ASP-DOWN to ASP-INACTIVE within a particular
AS, a Notify message SHOULD be sent, by the ASP-UP receptor, after
sending the ASP-UP-ACK, in order to inform the ASP of the current AS
state.

In the case where a Notify message ("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 is 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 M3UA peer may optionally send Heartbeat messages periodically,
subject to a provisionable timer T(beat). Upon receiving a Heartbeat
message, the M3UA peer MUST respond with a Heartbeat Ack message.

If no Heartbeat Ack message (or any other M3UA message) is received
from the M3UA peer within 2*T(beat), the remote M3UA 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
M3UA 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 M3UA 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 3 "ASP state
      transition diagram".

4.4 Routing Key Management Procedures [Optional]

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

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 determines that the requested RK partially, but not
exactly, matches an existing RK, and that an incoming signalling
message received at an SGP could possibly match both the requested
and the existing RK, 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 determines that the received RK was already registered,
fully and exactly, either statically or dynamically, by the sending
ASP, the SGP returns a Registration Response message to the ASP,
containing a Registration Result "Error - Routing Key Already
Registered ". This error applies whether the Routing Key is Active or
Inactive. For this error code, RC field in Registration Response
message MUST be populated with the actual value of RC in SGP
corresponding to the specified RK in Registration Request message.

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 "ERR - Routing Key
Change Refused" is returned if the SGP does not accept the
modification of the Routing Key due to either it does not support the
re-registration procedure or the specific RC does not exist.
Otherwise if the change is accepted, a Registration Response
"Successfully Registered" is returned.

If the SGP does not authorize an otherwise valid 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 a received Routing Key does not currently
exist, and the SGP supports dynamic configuration but requires that
the Routing Key first be manually provisioned at the SGP, 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 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.

A Registration Response "Error - Unsupported Traffic Handling Mode"

is returned if the Routing Key in the REG REQ contains an 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.

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
deregister. 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 deregistered as an ASP in the related
Application Server.

The deregistration procedure does not necessarily imply the deletion
of Routing Key and Application Server configuration data at the SG.
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
SG 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.

   For the IPSP SE model, it MAY be used one common RK for both IPSP
   participating in the communication using the Signaling Point Code
   granularity. It would basically consist of <OPC,DPC>. In the case of
   RC use, RCs SHOULD be previously agreed between both peers.

**4.5 Procedures to Support the Availability or Congestion Status of SS7
    Destination**

4.5.1 At an SGP

   On receiving an MTP-PAUSE, MTP-RESUME or MTP-STATUS indication
   primitive from the nodal interworking function at an SGP, the SGP
   M3UA layer will send a corresponding SS7 Signalling Network
   Management (SSNM) DUNA, DAVA, SCON, or DUPU message (see Section 3.4)
   to the M3UA peers at concerned ASPs. The M3UA layer must fill in
   various fields of the SSNM messages consistently with the information
   received in the primitives.

   The SGP M3UA 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.

   For the particular case that an ASP becomes active for an AS and
   destinations normally accessible to the AS are inaccessible,
   restricted or congested, the SG MAY send DUNA, DRST or SCON messages
   for the inaccessible, restricted or congested destinations to the ASP
   newly active for the AS to prevent the ASP from sending traffic for
   destinations that it might otherwise not know that are inaccessible,
   restricted or congested.

   DUNA, DAVA, SCON, and DRST messages may be sent sequentially and
   processed at the receiver in the order sent.

   Sequencing is not required for the DUPU or DAUD messages, which MAY
   be sent unsequenced.

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 M3UA Peer, the M3UA layer invokes the appropriate primitive indications to the resident M3UA-Users. Local management is informed.

In the case where a local event has caused the unavailability or congestion status of SS7 destinations, the M3UA layer at the ASP SHOULD pass up appropriate indications in the primitives to the M3UA 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. MTP-PAUSE indication primitives to the M3UA User are appropriate.

4.5.2.2 Multiple SG Configurations

At an ASP, upon receiving a Signalling Network Management message from the remote M3UA Peer, the M3UA 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 M3UA layer invokes the appropriate primitive indications to the resident M3UA-Users. Local management is informed.

Implementation Note: To accomplish this, the M3UA layer at an ASP maintains the status of routes via the SG, much like an MTP3 layer maintains route-set status.

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 Destination Point Codes.

The DAUD message MAY be sent unsequenced. The DAUD MAY be sent by the ASP 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 Codes. 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 MTP3
availability/congested status of the routeset associated with each
Destination Point Code(s) in the DAUD message. The status of each
SS7 destination 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). Where the SGP maintains the
congestion status of the SS7 destination, the SGP MUST additionally
respond with an SCON message before the DAVA or DRST message. If the
SS7 destination is available, the SGP MUST respond with an SCON
message (indicating the appropriate congestion level) and then a DAVA
message. If the SS7 destination is restricted, the SGP MUST respond
with an SCON message (with the appropriate congestion level)
immediately followed by a DRST message. If the SGP has no
information on the availability status of the SS7 destination, the
SGP responds with a DUNA message, as it has no routing information to
allow it to route traffic to this destination.

Where the SGP does not maintain the congestion status of the SS7
destination, the response to a DAUD message should always be only a
DAVA, DRST or DUNA message as appropriate.

Any DUNA or DAVA message in response to a DAUD message MAY contain a
list of Affected Point Codes.

An SG MAY refuse to provide the availability or congestion status of
a destination if, for example, the ASP is not authorized to know the
status of the destination. The SG MAY respond with an Error Message
(Error Code = "Destination 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 M3UA layers
at the SGPs inform all concerned ASPs in the ASP-ACTIVE state of any
available/restricted SS7 destinations using the DAVA/DRST messages.
No message is necessary for those destinations still unavailable
after the restart procedure.

When the M3UA layer at an ASP receives a DUNA message indicating SS7
destination unavailability at an SG, MTP Users will receive an MTP-
PAUSE indication and will stop any affected traffic to this
destination.   When the M3UA receives a DAVA/DRST message, MTP Users
will receive an MTP-RESUME indication and can resume traffic to the
newly available SS7 destination, 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 current
destination statuses. If MTP restart is 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.

When an ASP becomes active for an AS and the SG is experiencing SS7
network isolation or is performing the MTP Restart procedure for the
AS, the SG MAY send a DUNA message for the concerned destinations to
the newly active ASP to prevent the ASP from sending traffic.

In the IPSP case, MTP restart could be considered if the IPSP also
has connection to an SS7 network. In that case, the same behavior as
described above for the SGP would apply to the restarting IPSP. This
would also be the case if the IPSPs were perceived as exchanging MTP
Peer PDUs, instead of MTP primitives between MTP User and MTP
Provider. In other words, M3UA does not provide the equivalent to

Traffic Restart Allowed messages indicating the end of the restart
procedure between peer IPSPs that would also be connected to an SS7
network.

4.7 NIF not Available

IMPLEMENTATION NOTE: Although the NIF is decided to be an
implementation dependent function, here there are some guidelines
that may be useful to follow:

- If the SG (all the SGPs) is isolated from the NIF, then all the
  users are isolated from the SS7 network. A DUNA(*) message may be
  sent from the SGPs to all the ASPs.

Sidebottom,Morneault,Pastor

   - If only one SGP in the SG is isolated entirely from the NIF, the
     SGP may abort its associations. An alternative would be for the SGP
     to send ASP Down Ack.

   - If one or more SGP suffer a partial failure (where aborting the
     association(s) would cause all active AS(es) to fail), then the SGP
     may send DUNA messages for the affected SPC(es). This is the case
     where an SGP can continue to service one or more active AS(es), but
     due to a partial failure it is unable to service other(s) active
     AS(es).

4.8 M3UA Version Control

   If a 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 likely that the message
   having an unsupported version is an ASP Up message and therefore that
   the Error message would normally come from the SGP.

5. Examples of M3UA Procedures

5.1 Establishment of Association and Traffic between SGPs and ASPs

   These scenarios show the example M3UA message flows for the
   establishment of traffic between an SGP and an ASP or between two
   IPSPs. In all cases it is assumed that the SCTP association is
   already set up.

5.1.1 Single ASP in an Application Server ("1+0" sparing),

   These scenarios show the example M3UA message flows for the
   establishment of traffic between an SGP and an ASP where only one ASP
   is configured within an AS (no backup).

5.1.1.1 Single ASP in an Application Server ("1+0" sparing),
       No Registration

```
               SGP                                ASP1
                |                                  |
                |<-------------ASP Up-----------|
                |-----------ASP Up Ack--------->|
                |                                  |
                |-----NTFY(AS-INACTIVE)(RCn)--->|
```

```
            |                        |
            |<------- ASP Active(RCn)-------|   RC: Routing Context
```

```
                |-----ASP Active Ack (RCn)----->|     (optional)
                |                               |
                |-----NTFY(AS-ACTIVE)(RCn)----->|
                |                               |
```

   Note: If the ASP Active message contains an optional Routing Context
   parameter, the ASP Active message only applies for the specified RC
   value(s). For an unknown RC value, the SGP responds with an Error
   message.

5.1.1.2 Single ASP in Application Server ("1+0" sparing),
        Dynamic Registration

   This scenario is the same as for 5.1.1.1 but with the optional
   exchange of registration information. In this case the Registration
   is accepted by the SGP.

```
              SGP                             ASP1
               |                               |
               |<------------ASP Up------------|
               |----------ASP Up Ack---------->|
               |                               |
               |                               |
               |<----REGISTER REQ(LRCn,RKn)----|  LRC: Local Routing
               |                               |        Key Id
               |----REGISTER RESP(LRCn,RCn)--->|   RK: Routing Key
               |                               |   RC: Routing Context
               |----NTFY(AS-INACTIVE)(RCn)---->|
               |                               |
               |                               |
               |<------- ASP Active(RCn)-------|
               |-----ASP Active Ack (RCn)----->|
               |                               |
               |-----NTFY(AS-ACTIVE)(RCn)----->|
               |                               |
```

   Note: In the case of an unsuccessful registration attempt (e.g.,
   invalid RKn), the Register Response message will contain an
   unsuccessful indication and the ASP will not subsequently send an ASP
   Active message.

5.1.1.3 Single ASP in Multiple Application Servers (each
        with "1+0" sparing), Dynamic Registration (Case 1 - Multiple
        Registration Requests)

```
              SGP                             ASP1
               |                               |
               |<------------ASP Up------------|
```

```
              |----------ASP Up Ack---------->|
              |                               |
```

```
                |<----REGISTER REQ(LRC1,RK1)----|  LRC: Local Routing
                |                               |        Key Id
                |----REGISTER RESP(LRC1,RC1)--->|   RK: Routing Key
                |                               |   RC: Routing Context
                |---NOTIFY(AS-INACTIVE)(RC1)--->|
                |                               |
                |                               |
                |<------- ASP Active(RC1)-------|
                |-----ASP Active Ack (RC1)----->|
                |                               |
                |----NOTIFY(AS-ACTIVE)(RC1)---->|
                |                               |
                ~                               ~
                |                               |
                |<----REGISTER REQ(LRCn,RKn)----|
                |                               |
                |----REGISTER RESP(LRCn,RCn)--->|
                |                               |
                |                               |
                |<------- ASP Active(RCn)-------|
                |-----ASP Active Ack (RCn)----->|
                |                               |
                |----NOTIFY(AS-ACTIVE)(RCn)---->|
                |                               |
```

   Note: In the case of an unsuccessful registration attempt (e.g.,
   invalid RKn), the Register Response message will contain an
   unsuccessful indication and the ASP will not subsequently send an ASP
   Active message. Each LRC/RK pair registration is considered
   independently.

   It is not necessary to follow a Registration Request/Response message
   pair with an ASP Active message before sending the next Registration
   Request. The ASP Active message can be sent at any time after the
   related successful registration.

5.1.1.4 **Single ASP in Multiple Application Servers (each
   with "1+0" sparing), Dynamic Registration (Case 2 - Single
   Registration Request)**

```
                SGP                           ASP1
                 |                             |
                 |<-----------ASP Up-----------|
                 |----------ASP Up Ack--------->|
                 |                             |
                 |                             |
                 |<---REGISTER REQ({LRC1,RK1},  |
                 |                 ...,         |
```

```
                     |                {LRCn,RKn}),--|
                     |                              |
                     |---REGISTER RESP({LRC1,RC1},-->|
```

```
             |                      ...,               |
             |                   (LRCn,RCn})           |
             |                                         |
             |--NTFY(AS-INACTIVE)(RC1..RCn)->|
             |                                |
             |                                |
             |<------- ASP Active(RC1)-------|
             |-----ASP Active Ack (RC1)----->|
             |                                |
             |----NOTIFY(AS-ACTIVE)(RC1)---->|
             |                                |
             :                                :
             :                                :
             |                                |
             |<------- ASP Active(RCn)-------|
             |-----ASP Active Ack (RCn)----->|
             |                                |
             |----NOTIFY(AS-ACTIVE)(RCn)---->|
             |                                |
```

   Note: In the case of an unsuccessful registration attempt (e.g.,
   Invalid RKn), the Register Response message will contain an
   unsuccessful indication and the ASP will not subsequently send an ASP
   Active message. Each LRC/RK pair registration is considered
   independently.

   The ASP Active message can be sent at any time after the related
   successful registration, and may have more than one RC.

5.1.2 Two ASPs in Application Server ("1+1" sparing)

   This scenario shows the example M3UA message flows for the
   establishment of traffic between an SGP and two ASPs in the same
   Application Server, where ASP1 is configured to be in the ASP-ACTIVE
   state and ASP2 is to be a "backup" in the event of communication
   failure or the withdrawal from service of ASP1. ASP2 may act as a
   hot, warm, or cold backup depending on the extent to which ASP1 and
   ASP2 share call/transaction state or can communicate call state under
   failure/withdrawal events. The example message flow is the same
   whether the ASP Active messages indicate "Override", "Loadshare" or
   "Broadcast" mode, although typically this example would use an
   Override mode.

```
          SGP                        ASP1                      ASP2
           |                          |                         |
           |<--------ASP Up---------|                         |
           |-------ASP Up Ack------>|                         |
           |                          |                         |
```

```
        |--NOTIFY(AS-INACTIVE)-->|                        |
        |                        |                        |
        |<-----------------------ASP Up----------------|
```

```
        |--------------------------ASP Up Ack------------>|
        |                         |                       |
        |                         |                       |
        |<-------ASP Active------|                       |
        |------ASP Active Ack--->|                       |
        |                         |                       |
        |---NOTIFY(AS-ACTIVE)--->|                       |
        |------------------------NOTIFY(AS-ACTIVE)------->|
        |                         |                       |
```

5.1.3 **Two ASPs in an Application Server ("1+1" sparing,
        loadsharing case)**

   This scenario shows a similar case to Section 5.1.2 but where the two
   ASPs are brought to the state ASP-ACTIVE and subsequently loadshare
   the traffic. In this case, one ASP is sufficient to handle the total
   traffic load.

```
          SGP                      ASP1                    ASP2
           |                        |                       |
           |<---------ASP Up--------|                       |
           |--------ASP Up Ack----->|                       |
           |                        |                       |
           |--NOTIFY(AS-INACTIVE)-->|                       |
           |                        |                       |
           |<--------------------------ASP Up--------------|
           |--------------------------ASP Up Ack---------->|
           |                        |                       |
           |<--ASP Active (Ldshr)---|                       |
           |-----ASP-Active Ack---->|                       |
           |                        |                       |
           |---NOTIFY (AS-ACTIVE)-->|                       |
           |----------------------------NOTIFY(AS-ACTIVE)---->|
           |                        |                       |
           |<--------------------------ASP Active (Ldshr)-----|
           |--------------------------ASP Active Ack------>|
           |                        |                       |
```

5.1.4 **Three ASPs in an Application Server ("n+k" sparing,
   loadsharing case)**

   This scenario shows the example M3UA message flows for the
   establishment of traffic between an SGP and three ASPs in the same
   Application Server, where two of the ASPs are brought to the state
   ASP-ACTIVE and subsequently share the load. In this case, a minimum
   of two ASPs are required to handle the total traffic load (2+1
   sparing).

```
        SGP                 ASP1                ASP2                ASP3
         |                   |                   |                   |
```

```
            |<------ASP Up------|                    |                    |
            |-----ASP Up Ack--->|                    |                    |
            |                    |                    |                    |
            |<------------------------ASP Up-------|                      |
            |----------------------ASP Up Ack---->|                       |
            |                    |                    |                    |
            |NTFY(AS-INACTIVE)->|                    |                    |
            |-----------------NOTIFY(AS-INACTIVE)->|                      |
            |                    |                    |                    |
            |<----------------------------------------------ASP Up--------|
            |----------------------------------------------ASP Up Ack---->|
            |                    |                    |                    |
            |                    |                    |                    |
            |<--ASP Act (Ldshr)-|                    |                    |
            |----ASP Act Ack--->|                    |                    |
            |                    |                    |                    |
            |                    |                    |                    |
            |<------------------ASP Act. (Ldshr)---|                      |
            |---------------------ASP Act Ack----->|                      |
            |                    |                    |                    |
            |--NTFY(AS-ACTIVE)->|                    |                    |
            |-------------------NOTIFY(AS-ACTIVE)->|                      |
            |-----------------------------------------NOTIFY(AS-ACTIVE)->|
            |                    |                    |                    |
            |                    |                    |                    |
```

5.2 ASP Traffic Failover Examples

5.2.1 (1+1 Sparing, Withdrawal of ASP, Backup Override)

   Following on from the example in Section 5.1.2, and ASP1 withdraws
   from service:

```
            SGP                    ASP1                    ASP2
             |                      |                       |
             |<-----ASP Inactive------|                     |
             |----ASP Inactive Ack--->|                     |
             |                      |                       |
             |----NTFY(AS-PENDING)--->|                     |
             |----------------------NTFY(AS-PENDING)----------->|
             |                      |                       |
             |<---------------------------- ASP Active----------|
             |----------------------------ASP Active Ack------->|
             |                      |                       |
             |----NTFY(AS-ACTIVE)---->|                     |
             |----------------------NTFY(AS-ACTIVE)------------>|
```

   Note: If the SGP M3UA layer detects the loss of the M3UA peer (e.g.,

M3UA heartbeat loss or detection of SCTP failure), the initial ASP
Inactive message exchange (i.e., SGP to ASP1) would not occur.

5.2.2 (1+1 Sparing, Backup Override)

Following on from the example in Section 5.1.2, ASP2 wishes to
Override ASP1 and take over the traffic:

```
         SGP                           ASP1                        ASP2
          |                             |                           |
          |<---------------------------- ASP Active----------|
          |----------------------------ASP Active Ack------>|
          |----NTFY(Alt ASP-Act)-->|
          |                             |                           |
```

5.2.3 (n+k Sparing, Loadsharing case, Withdrawal of ASP)

Following on from the example in Section 5.1.4, and ASP1 withdraws
from service:

```
     SGP                    ASP1                   ASP2                   ASP3
      |                      |                      |                      |
      |<----ASP Inact.----|                      |                      |
      |---ASP Inact Ack-->|                      |                      |
      |                      |                      |                      |
      |--NTFY(Ins. ASPs)->|                      |                      |
      |--------------------------------------NOTIFY(Ins. ASPs)-->|
      |                      |                      |                      |
      |                      |                      |                      |
      |<--------------------------------------ASP Act (Ldshr)---|
      |--------------------------------------ASP Act (Ack)--->|
      |                      |                      |                      |
      |-NTFY(AS-ACTIVE)-->|                      |                      |
      |------------------NOTIFY(AS-ACTIVE)-->|                      |
      |--------------------------------------NOTIFY(AS-ACTIVE)-->|
      |                      |                      |                      |
      |                      |                      |                      |
```
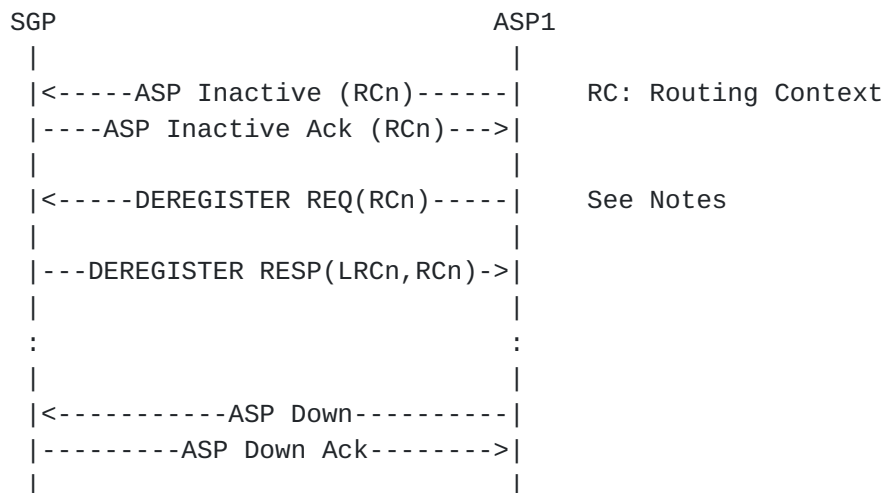
For the Notify message to be sent, the SG maintains knowledge of the
minimum ASP resources required (e.g., if the SG knows that "n+k" =
"2+1" for a Loadshare AS and "n" currently equals "1").

Note: If the SGP detects loss of the ASP1 M3UA peer (e.g., M3UA
heartbeat loss or detection of SCTP failure), the initial ASP
Inactive message exchange (i.e., SGP-ASP1) would not occur.

5.3 Normal Withdrawal of an ASP from an Application Server
   and Teardown of an Association

An ASP which is now confirmed in the state ASP-INACTIVE (i.e., the
ASP has received an ASP Inactive Ack message) may now proceed to the
ASP-DOWN state, if it is to be removed from service. Following on

from Section 5.2.1 or 5.2.3, where ASP1 has moved to the "Inactive"
state:

```
        SGP                              ASP1
         |                                |
         |<-----ASP Inactive (RCn)------|    RC: Routing Context
         |----ASP Inactive Ack (RCn)--->|
         |                                |
         |<-----DEREGISTER REQ(RCn)-----|    See Notes
         |                                |
         |---DEREGISTER RESP(LRCn,RCn)->|
         |                                |
         :                                :
         |                                |
         |<-----------ASP Down----------|
         |---------ASP Down Ack-------->|
         |                                |
```

Note: The Deregistration procedure will typically be used if the ASP
previously used the Registration procedures for configuration within
the Application Server. ASP Inactive and Deregister messages
exchanges may contain multiple Routing Contexts.

The ASP should be in the ASP-INACTIVE state and should have
deregistered in all its Routing Contexts before attempting to move to
the ASP-DOWN state.

5.4 Auditing examples

5.4.1 SG State: Uncongested / Available

```
        ASP                            SGP
        ---                            ---
         |   -------- DAUD --------->  |
         |   <------ SCON(0) --------  |
         |   <------- DAVA ----------  |
```


5.4.2 SG state: Congested (Congestion Level=2) / Available

```
        ASP                            SGP
        ---                            ---
         |   -------- DAUD --------->  |
         |   <------ SCON(2) --------  |
         |   <------- DAVA ----------  |
```


5.4.3 SG state: Unknown / Available

ASP   SGP

```
      ---                              ---
       |  -------- DAUD --------->  |
       |  <------- DAVA ----------  |
```

5.4.4 SG state: Unavailable

```
      ASP                              SGP
      ---                              ---
       |  -------- DAUD --------->  |
       |  <------- DUNA ----------  |
```

5.5 M3UA/MTP3-User Boundary Examples

5.5.1 At an ASP

   This section describes the primitive mapping between the MTP3 User
   and the M3UA layer at an ASP.

5.5.1.1 Support for MTP-TRANSFER Primitives at the ASP

5.5.1.1.1 Support for MTP-TRANSFER Request Primitive

   When the MTP3-User on the ASP has data to send to a remote MTP3-User,
   it uses the MTP-TRANSFER request primitive. The M3UA layer at the
   ASP will do the following when it receives an MTP-TRANSFER request
   primitive from the M3UA user:

      - Determine the correct SGP;

      - Determine the correct association to the chosen SGP;

      - Determine the correct stream in the association (e.g.,
        based on SLS);

      - Determine whether to complete the optional fields of the DATA
        message;

      - Map the MTP-TRANSFER request primitive into the Protocol Data
        field of a DATA message;

      - Send the DATA message to the remote M3UA peer at the SGP,
        over the SCTP association.

```
          SGP                       ASP
           |                         |
           |<-----DATA Message-------|<--MTP-TRANSFER req.
```
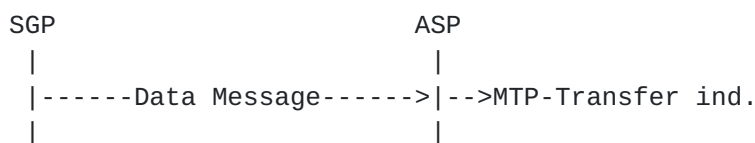
Sidebottom,Morneault,Pastor

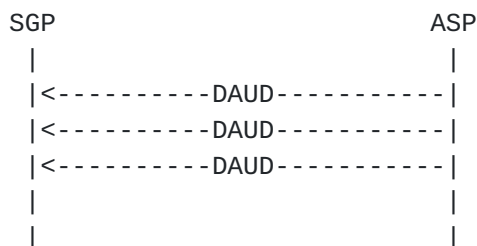**5.5.1.1.2** **Support for the MTP-TRANSFER Indication Primitive**

When the M3UA layer on the ASP receives a DATA message from the M3UA
peer at the remote SGP, it will do the following:

   - Evaluate the optional fields of the DATA message, if present;

   - Map the Protocol Data field of a DATA message into the
     MTP-TRANSFER indication primitive;

   - Pass the MTP-TRANSFER indication primitive to the user part. In
     case of multiple user parts, the optional fields of the Data
     message are used to determine the concerned user part.

```
        SGP                        ASP
         |                          |
         |------Data Message------>|-->MTP-Transfer ind.
         |                          |
```

5.5.1.1.3 **Support for ASP Querying of SS7 Destination States**

There are situations such as temporary loss of connectivity to the
SGP that may cause the M3UA layer at the ASP to audit SS7 destination
availability/congestion states. Note: there is no primitive for the
MTP3-User to request this audit from the M3UA layer as this is
initiated by an internal M3UA management function.

```
        SGP                             ASP
         |                               |
         |<----------DAUD-----------|
         |<----------DAUD-----------|
         |<----------DAUD-----------|
         |                               |
         |                               |
```

5.5.2 **At an SGP**

This section describes the primitive mapping between the MTP3-User
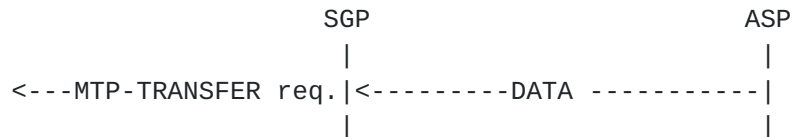and the M3UA layer at an SGP.

5.5.2.1 **Support for MTP-TRANSFER Request Primitive at the SGP**

When the M3UA layer at the SGP has received DATA messages from its
peer destined to the SS7 network it will do the following:

   - Evaluate the optional fields of the DATA message, if present, to
     determine the Network Appearance;

- Map the Protocol data field of the DATA message into an
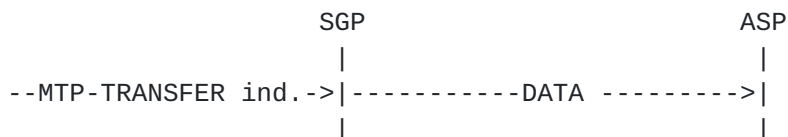   MTP-TRANSFER request primitive;

        - Pass the MTP-TRANSFER request primitive to the MTP3 of the
          concerned Network Appearance.

```
                         SGP                           ASP
                          |                             |
         <---MTP-TRANSFER req.|<---------DATA -----------|
                          |                             |
```

5.5.2.2 Support for MTP-TRANSFER Indication Primitive at the SGP

   When the MTP3 layer at the SGP has data to pass its user parts, it
   will use the MTP-TRANSFER indication primitive. The M3UA layer at
   the SGP will do the following when it receives an MTP-TRANSFER
   indication primitive:

      - Determine the correct AS using the distribution function;

      - Select an ASP in the ASP-ACTIVE state

      - Determine the correct association to the chosen ASP;

      - Determine the correct stream in the SCTP association (e.g.,
        based on SLS);

      - Determine whether to complete the optional fields of the DATA
        message;

      - Map the MTP-TRANSFER indication primitive into the Protocol Data
        field of a DATA message;

      - Send the DATA message to the remote M3UA peer in the ASP, over
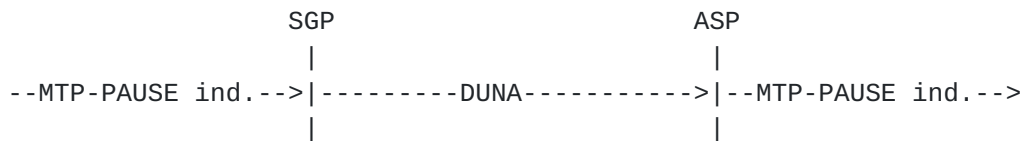   the SCTP association

```
                         SGP                           ASP
                          |                             |
         --MTP-TRANSFER ind.->|-----------DATA --------->|
                          |                             |
```

**5.5.2.3 Support for MTP-PAUSE, MTP-RESUME, MTP-STATUS Indication
         Primitives**

   The MTP-PAUSE, MTP-RESUME and MTP-STATUS indication primitives from
   the MTP3 upper layer interface at the SGP need to be made available
   to the remote MTP3 User Part lower layer interface at the concerned
   ASP(s).

5.5.2.3.1 Destination Unavailable

The MTP3 layer at the SGP will generate an MTP-PAUSE indication
primitive when it determines locally that an SS7 destination is

unreachable. The M3UA layer will map this primitive to a DUNA
message. The SGP M3UA layer determines the set of concerned ASPs to
be informed based on internal SS7 network information associated with
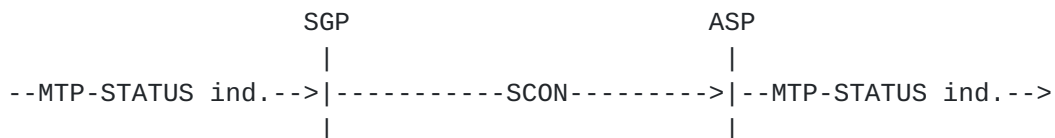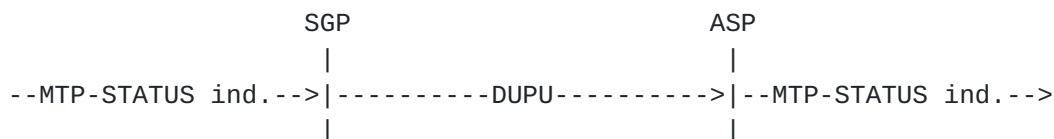the MTP-PAUSE indication primitive indication.

```
                    SGP                        ASP
                     |                          |
   --MTP-PAUSE ind.-->|---------DUNA----------->|--MTP-PAUSE ind.-->
                     |                          |
```

5.5.2.3.2 Destination Available

The MTP3 at the SGP will generate an MTP-RESUME indication primitive
when it determines locally that an SS7 destination that was
previously unreachable is now reachable. The M3UA layer will map
this primitive to a DAVA message. The SGP M3UA determines the set of
concerned ASPs to be informed based on internal SS7 network
information associated with the MTP-RESUME indication primitive.

```
                    SGP                        ASP
                     |                          |
   --MTP-RESUME ind.-->|-----------DAVA--------->|--MTP-RESUME ind.-->
                     |                          |
```

5.5.2.3.3 SS7 Network Congestion

The MTP3 layer at the SGP will generate an MTP-STATUS indication
primitive when it determines locally that the route to an SS7
destination is congested. The M3UA layer will map this primitive to
a SCON message. It will determine which ASP(s) to send the SCON
message to, based on the intended Application Server.

```
                    SGP                        ASP
                     |                          |
   --MTP-STATUS ind.-->|-----------SCON--------->|--MTP-STATUS ind.-->
                     |                          |
```

5.5.2.3.4 Destination User Part Unavailable

The MTP3 layer at the SGP will generate an MTP-STATUS indication
primitive when it receives an UPU message from the SS7 network. The
M3UA layer will map this primitive to a DUPU message. It will
determine which ASP(s) to send the DUPU based on the intended
Application Server.

```
                    SGP                        ASP
                     |                          |
   --MTP-STATUS ind.-->|----------DUPU---------->|--MTP-STATUS ind.-->
                     |                          |
```

[5.6](#) **Examples for IPSP communication.**

These scenarios show a basic example for IPSP communication for the
three phases of the connection (establishment, data exchange,
disconnection). It is assumed that the SCTP association is already
set up. Both single exchange and double exchange behavior are
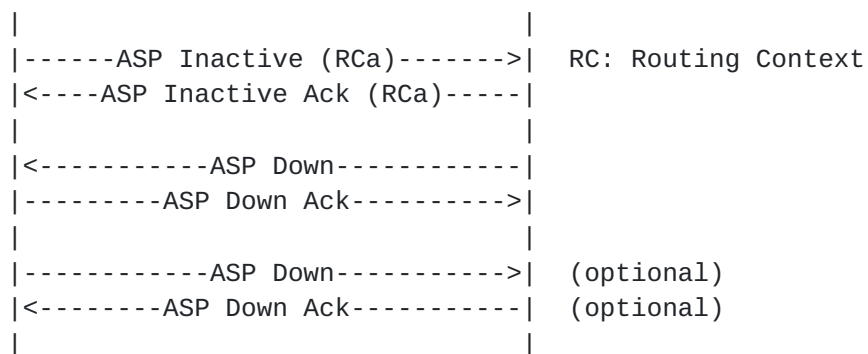included for illustrative purposes.

5.6.1 Single exchange:

```
        IPSP-A                         IPSP-B
          |                              |
          |------------ASP Up----------->|
          |<----------ASP Up Ack---------|
          |                              |
          |<------- ASP Active(RCb)-------|  RC: Routing Context
          |-----ASP Active Ack (RCb)----->|      (optional)
          |                              |
          |                              |
          |<========  DATA (RCb) ========>|
          |                              |
          |<-----ASP Inactive (RCb)-------|  RC: Routing Context
          |----ASP Inactive Ack (RCb)---->|      (optional)
          |                              |
          |<-----------ASP Down-----------|
          |---------ASP Down Ack--------->|
             |                              |
```

Routing Context are previously agreed to be the same in both
directions.

5.6.2 Double exchange:

```
        IPSP-A                         IPSP-B
          |                              |
          |<------------ASP Up-----------|
          |----------ASP Up Ack---------->|
          |                              |
          |------------ASP Up----------->|  (optional)
          |<----------ASP Up Ack---------|  (optional)
          |                              |
          |<------- ASP Active(RCb)-------|  RC: Routing Context
          |-----ASP Active Ack (RCb)----->|      (optional)
          |                              |
          |------- ASP Active(RCa)------->|  RC: Routing Context
          |<-----ASP Active Ack (RCa)-----|      (optional)
          |                              |
          |<========  DATA (RCa) ========|
          |=========  DATA (RCb) ========>|
```

```
        |                         |
        |<-----ASP Inactive (RCb)--------|  RC: Routing Context
        |----ASP Inactive Ack (RCb)----->|
```

```
            |                         |
            |------ASP Inactive (RCa)------->|   RC: Routing Context
            |<----ASP Inactive Ack (RCa)-----|
            |                         |
            |<-----------ASP Down-----------|
            |---------ASP Down Ack---------->|
            |                         |
            |-----------ASP Down----------->|   (optional)
            |<-------ASP Down Ack-----------|   (optional)
            |                         |
```

In this approach, only one single exchange of ASP Up message can be
considered as enough since the response by the other peer can be
considered as a notice that it is in ASP_UP state.

For the same reason, only one ASP Down message is needed since once
that an IPSP receives ASP_Down ack message it is itself considered as
being in the ASP_Down state and not allowed to receive ASPSM
messages.

6. Security Considerations

6.1 Introduction

M3UA is designed to carry signalling messages for telephony services.
As such, M3UA must involve the security needs of several parties: the
end users of the services; the network providers and the applications
involved. Additional requirements may come from local regulation.
While having some overlapping security needs, any security solution
should fulfill all of the different parties' needs.

6.2 Threats

There is no quick fix, one-size-fits-all solution for security. As a
transport protocol, M3UA has the following security objectives:

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

M3UA is recommended to be transported on SCTP. SCTP [17] provides
certain transport related security features, such as some protection
against:

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

When M3UA 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" [22] should be consulted for guidance.

When the network in which M3UA 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 [23] for more information on configuring IPSEC services.

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 [24] SHOULD
be used instead. Regardless of which level performs the encryption,
the IPSEC ISAKMP [25] service SHOULD be used for key management.

7. IANA Considerations

7.1 SCTP Payload Protocol Identifier

IANA has assigned an M3UA value for the Payload Protocol Identifier
in the SCTP DATA chunk. The following SCTP Payload Protocol
Identifier is registered:

        M3UA   "3"

The SCTP Payload Protocol Identifier value "3" SHOULD be included in
each SCTP DATA chunk, to indicate that the SCTP is carrying the M3UA
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 M3UA Port Number

IANA has registered SCTP (and UDP/TCP) Port Number 2905 for M3UA. 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 M3UA 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, and

-- 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 Guidelines for Writing an IANA Considerations Section in
RFCs (25]

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

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 new message class;
    (b) A detailed description of the purpose of the message class.

7.3.2 IETF Defined Message Types

The documentation for a new message type MUST include 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 for 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 ("Unsupported
Message Type").

7.3.3 IETF Defined 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 in Section 3.2;
    (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.

8. References

8.1 Normative References

[1]   ITU-T Recommendations Q.761 to Q.767, "Signalling System No.7
      (SS7) - ISDN User Part (ISUP)"

[2]   ANSI T1.113 - "Signaling System Number 7 - ISDN User Part"

[3]   ETSI ETS 300 356-1 "Integrated Services Digital Network (ISDN);
      Signalling System No.7; ISDN User Part (ISUP) version 2 for the
      international interface; Part 1: Basic services"

[4]   ITU-T Recommendations Q.711 to Q.715, "Signalling System No. 7
      (SS7) - Signalling Connection Control Part (SCCP)"

[5]   ANSI T1.112 "Signaling System Number 7 - Signaling Connection
      Control Part"

[6]   ETSI ETS 300 009-1, "Integrated Services Digital Network (ISDN);
      Signalling System No.7; Signalling Connection Control Part
      (SCCP) (connectionless and connection-oriented class 2) to
      support international interconnection; Part 1: Protocol
      specification"

[7]   ITU-T Recommendations Q.700 to Q.705, "Signalling System No. 7
      (SS7) - Message Transfer Part (MTP)"

[8]   ANSI T1.111 "Signaling System Number 7 - Message Transfer Part"

[9]   ETSI ETS 300 008-1, "Integrated Services Digital Network (ISDN);
      Signalling System No.7; Message Transfer Part (MTP) to support
      international interconnection; Part 1: Protocol specification"

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

8.2 Informative References

[11] Ong, L., Rytina, M., Garcia, H., Schwarzbauer, L., Coene, H.,
      Lin, I., Juhasz, M. and C. Holdrege, "Framework Architecture for
      Signaling Transport", RFC 2719, October 1999.

[12] ITU-T Recommendation Q.720, "Telephone User Part"

[13] ITU-T Recommendations Q.771 to Q.775 "Signalling System No. 7
      (SS7) - Transaction Capabilities (TCAP)"

    [14] ANSI T1.114 "Signaling System Number 7 - Transaction
         Capabilities Application Part"

Sidebottom,Morneault,Pastor

[15] ETSI ETS 300 287-1, "Integrated Services Digital Network (ISDN);
     Signalling System No.7; Transaction Capabilities (TC) version 2;
     Part 1: Protocol specification"

[16] 3G TS 25.410 V4.0.0 (2001-04) "Technical Specification - 3rd
     Generation partnership Project; Technical Specification Group
     Radio Access Network; UTRAN Iu Interface: General Aspects and
     Principles"

[17] Stewart, R., Xie, Q., Mornmeault, K., Sharp, H., Taylor, T.,
     Rytina, I., Kalla, M., Zhang, L. and V. Paxson, "Stream Control
     Transport Protocol", RFC 2960, October 2000.

[18] ITU-T Recommendation Q.2140 "B-ISDN ATM Adaptation Layer -
     Service Specific Coordination Function for signalling at the
     Network Node Interface (SSCF at NNI)"

[19] ITU-T Recommendation Q.2110 "B-ISDN ATM Adaptation Layer -
     Service Specific Connection Oriented Protocol (SSCOP)"

[20] Bradner, S., "Key words for use in RFCs to Indicate Requirement
     Levels", BCP 14, RFC 2119, March 1997.

[21] ITU-T Recommendation Q.2210 "Message Transfer Part Level 3
     functions and messages using the services of ITU Recommendation
     Q.2140"

[22] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September
     1997.

[23] Ramakrishnan, S., Floyd, S. and D. Black, "Security Architecture
     for the Internet Protocol", RFC 3168, November 1998.

[24] Kent, S. and R. Atkinson, "IP Encapsulating Security Payload
     (ESP)", RFC 2406, November 1998.

[25] Maughan, D., Schertler, M., Schneider, M. and J. Turner,
     "Internet Security Association and Key Management Protocol", RFC
     2408, November 1998.

[26] Narten, T. and H. Alverstrand, "Guidelines for Writing an IANA
     Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[27] Morneault, K., Dantu, R., Sidebottom, G., Bidulock, B. and J.
     Heitz, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2)
     - User Adaptation Layer", RFC 3331, August 2002.

[28] George, T., et. al., "SS7 MTP2-User Peer-to-Peer Adaptation

Layer", Work in Progress.

    [29] Telecommunication Technology Committee (TTC) Standard JT-Q704,
         "Message Transfer Part Signaling Network Functions", April 28,
         1992.

9. Acknowledgements

The authors would like to thank Antonio Roque Alvarez, Joyce
Archibald, Tolga Asveren, Maria-Cruz Bartolome-Rodrigo, Dan Brendes,
Antonio Canete, Nikhil Jain, Roland Jesske, Joe Keller, Kurt Kite,
Ming Lin, Steve Lorusso, Naoto Makinae, Howard May, Francois
Mouillaud, Barry Nagelberg, Neil Olson, Heinz Prantner, Shyamal
Prasad, Mukesh Punhani, Selvam Rengasami, John Schantz, Ray Singh,
Michael Tuexen, Nitin Tomar, Gery Verwimp, Tim Vetter, Kazuo
Watanabe, Ben Wilson and many others for their valuable comments and
suggestions.

10. Document Contributors

    Ian Rytina - Ericsson
    Guy Mousseau - Nortel Networks
    Lyndon Ong - Ciena
    Hanns Juergen Schwarzbauer - Siemens
    Klaus Gradischnig - Detecon Inc.
    Mallesh Kalla - Telcordia
    Normand Glaude - Performance Technologies
    Brian Bidulock - OpenSS7
    John Loughney - Nokia

Appendix A

A.1 Signalling Network Architecture

A Signalling Gateway is used to support the transport of MTP3-User
signalling traffic received from the SS7 network to multiple
distributed ASPs (e.g., MGCs and IP Databases). Clearly, the M3UA
protocol is not designed to meet the performance and reliability
requirements for such transport by itself. However, the conjunction
of distributed architecture and redundant networks provides support
for reliable transport of signalling traffic over IP. The M3UA
protocol is flexible enough to allow its operation and management in
a variety of physical configurations, enabling Network Operators to
meet their performance and reliability requirements.

To meet the stringent SS7 signalling reliability and performance
requirements for carrier grade networks, Network Operators might
require that no single point of failure is present in the end-to-end
network architecture between an SS7 node and an IP-based application.
This can typically be achieved through the use of redundant SGPs or

SGs, redundant hosts, and the provision of redundant QOS-bounded IP
network paths for SCTP Associations between SCTP End Points.

Obviously, the reliability of the SG, the MGC and other IP-based
functional elements also needs to be taken into account. The
distribution of ASPs and SGPs within the available Hosts MAY also be
considered. As an example, for a particular Application Server, the
related ASPs could be distributed over at least two Hosts.

One example of a physical network architecture relevant to SS7
carrier grade operation in the IP network domain is shown in Figure 5
below:

```
          SGs                                       MGCs


Host#1 **************                        ************** Host#3
       *   ********__*_____*__********   *    =
       *   *SGP1.1*__*_____              _____*__* ASP1 *   *   MGC1
       *   ********   *      \      /             *   ********   *
       *   ********__*_____/_____*_ ********   *
       *   *SGP2.1*__*_____\/_____      _____*__* ASP2 *   *
       *   ********   *        /\       |    |   *   ********   *
       *      :      *       /  \      |    |   *      :       *
       *   ********   *     /    \     |    |   *   ********   *
       *   * SGPn *   *    |    |    |    |   *   * ASPn *   *
       *   ********   *    |    |    |    |   *   ********   *
       **************      |    |    |    |   **************
                          |    |   \    /
                          |    |    \  /
Host#2 **************      |    |     \ /        ************** Host#4
       *   ********__*_____|    |_____\/_____*__********   *    =
       *   *SGP1.2*__*_____/_____*__* ASP1 *   *   MGC2
       *   ********   *              /  \       *   ********   *
       *   ********__*_____/    \_____*__********   *
       *   *SGP2.2*__*_____*__* ASP2 *   *
       *   ********   *                          *   ********   *
       *      :      *     SCTP Associations     *      :       *
       *   ********   *                          *   ********   *
       *   * SGPn *   *                          *   * ASPn *   *
       *   ********   *                          *   ********   *
       **************                            **************
```

SGP1.1 and SGP1.2 are part of SG1
SGP2.1 and SGP2.2 are part of SG2

                    Figure 5 - Physical Model

In this model, each host may have many application processes. In the
case of the MGC, an ASP may provide service to one or more
Application Servers, and is identified as an SCTP end point. One or
more Signalling Gateway Processes make up a single Signalling
Gateway.

This example model can also be applied to IPSP-IPSP signalling. In
this case, each IPSP may have its services distributed across 2 hosts

or more, and may have multiple server processes on each host.

In the example above, each signalling process (SGP, ASP or IPSP) is
the end point to more than one SCTP association, leading to more than
one other signalling processes. To support this, a signalling
process must be able to support distribution of M3UA messages to many
simultaneous active associations. This message distribution function
is based on the status of provisioned Routing Keys, the status of the
signalling routes to signalling points in the SS7 network, and the
redundancy model (active-standby, load sharing, broadcast, n+k) of
the remote signalling processes.

For carrier grade networks, the failure or isolation of a particular
signalling process should not cause stable calls or transactions to
be lost. This implies that signalling processes need, in some cases,
to share the call/transaction state or be able to pass the call state
information between each other. In the case of ASPs performing call
processing, coordination may also be required with the related Media
Gateway to transfer the MGC control for a particular trunk
termination. However, this sharing or communication of
call/transaction state information is outside the scope of this
document.

This model serves as an example. M3UA imposes no restrictions as to
the exact layout of the network elements, the message distribution
algorithms and the distribution of the signalling processes.
Instead, it provides a framework and a set of messages that allow for
a flexible and scalable signalling network architecture, aiming to
provide reliability and performance.

A.2 Redundancy Models

A.2.1 Application Server Redundancy

At the SGP, an Application Server list contains active and inactive
ASPs to support ASP broadcast, loadsharing and failover procedures.
The list of ASPs within a logical Application Server is kept updated
in the SGP to reflect the active Application Server Process(es).

For example, in the network shown in Figure 1, all messages to DPC x
could be sent to ASP1 in Host3 or ASP1 in Host4. The AS list at SGP1
in Host 1 might look like the following:

```
   Routing Key {DPC=x) - "Application Server #1"
      ASP1/Host3  - State = Active
      ASP1/Host4  - State = Inactive
```

In this "1+1" redundancy case, ASP1 in Host3 would be sent any
incoming message with DPC=x. ASP1 in Host4 would normally be brought

to the "active" state upon failure of, or loss of connectivity to,
ASP1/Host1.

The AS List at SGP1 in Host1 might also be set up in loadshare mode:

```
Routing Key {DPC=x) - "Application Server #1"
    ASP1/Host3 - State = Active
    ASP1/Host4 - State = Active
```

In this case, both the ASPs would be sent a portion of the traffic.
For example the two ASPs could together form a database, where
incoming queries may be sent to any active ASP.

Care might need to be exercised by a Network Operator in the
selection of the routing information to be used as the Routing Key
for a particular AS.

In the process of failover, it is recommended that in the case of
ASPs supporting call processing, stable calls do not fail. It is
possible that calls in "transition" may fail, although measures of
communication between the ASPs involved can be used to mitigate this.

For example, the two ASPs may share call state via shared memory, or
may use an ASP to ASP protocol to pass call state information. Any
ASP-to-ASP protocol to support this function is outside the scope of
this document.

A.2.2 Signalling Gateway Redundancy

Signalling Gateways may also be distributed over multiple hosts.
Much like the AS model, SGs may comprise one or more SG Processes
(SGPs), distributed over one or more hosts, using an active/backup or
a loadsharing model. Should an SGP lose all or partial SS7
connectivity and other SGPs exist, the SGP may terminate the SCTP
associations to the concerned ASPs.

It is therefore possible for an ASP to route signalling messages
destined to the SS7 network using more than one SGP. In this model,
a Signalling Gateway is deployed as a cluster of hosts acting as a
single SG. A primary/backup redundancy model is possible, where the
unavailability of the SCTP association to a primary SGP could be used
to reroute affected traffic to an alternate SGP. A loadsharing model
is possible, where the signalling messages are loadshared between
multiple SGPs. A broadcast model is also possible, where signalling
messages are sent to each active SGP in the SG. The distribution of
the MTP3-user messages over the SGPs should be done in such a way to
minimize message missequencing, as required by the SS7 User Parts.

It may also be possible for an ASP to use more than one SG to access
a specific SS7 end point, in a model that resembles an SS7 STP mated
pair. Typically, SS7 STPs are deployed in mated pairs, with traffic

loadshared between them. Other models are also possible, subject to
the limitations of the local SS7 network provisioning guidelines.

From the perspective of the M3UA layer at an ASP, a particular SG is
capable of transferring traffic to a provisioned SS7 destination X if
an SCTP association with at least one SGP of the SG is established,
the SGP has returned an acknowledgement to the ASP to indicate that
the ASP is actively handling traffic for that destination X, the SGP
has not indicated that the destination X is inaccessible and the SGP
has not indicated MTP Restart. When an ASP is configured to use
multiple SGPs for transferring traffic to the SS7 network, the ASP
must maintain knowledge of the current capability of the SGPs to
handle traffic to destinations of interest. This information is
crucial to the overall reliability of the service, for active/backup,
loadsharing and broadcast models, in the event of failures, recovery
and maintenance activities. The ASP M3UA may also use this
information for congestion avoidance purposes. The distribution of
the MTP3-user messages over the SGPs should be done in such a way to
minimize message missequencing, as required by the SS7 User Parts.

Appendix B: Changes from [RFC3332](RFC3332)

outline any backward compatibility issues

Editors' Addresses

Greg Sidebottom
Signatus Technologies
Kanata, Ontario, Canada

EMail: greg@signatustechnologies.com

Ken Morneault
Cisco Systems Inc.
13615 Dulles Technology Drive
Herndon, VA, USA 20171

EMail: kmorneau@cisco.com

Javier Pastor-Balbas
Ericsson Espana S.A.
C/ Retama 1
28045 Madrid - Spain

EMail: j.javier.pastor@ericsson.com

Sidebottom,Morneault,Pastor

Full Copyright Statement

   Acknowledgment