

Network Working Group
INTERNET-DRAFT

Ken Morneault
Cisco Systems
Mallesh Kalla
Telcordia
Greg Sidebottom
Nortel Networks
Ram Dantu
IPMobile
Tom George
Alcatel

Expires in six months

March 2000

SS7 MTP2-User Adaptation Layer
<[draft-ietf-sigtran-m2ua-04.txt](#)>

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC 2026](#). Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as 'work in progress.'

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

To learn the current status of any Internet-Draft, please check the '1id-abstracts.txt' listing contained in the Internet- Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ftp.ietf.org (US East Coast), or ftp.isi.edu (US West Coast).

Abstract

This Internet Draft defines a protocol for backhauling of SS7 MTP2 User signaling messages over IP using the Simple Control Transmission

Protocol (SCTP). This protocol would be used between a Signaling Gateway (SG) and Media Gateway Controller (MGC). It is assumed that the SG receives SS7 signaling over a standard SS7 interface using the SS7 Message Transfer Part (MTP) to provide transport. The Signaling Gateway would act as a Signaling Link Terminal.

TABLE OF CONTENTS

1.	Introduction.....	2
1.1	Scope.....	2
1.2	Terminology.....	3
1.3	Signaling Transport Architecture.....	3
1.4	Services Provide by the M2UA Adaptation Layer.....	6
1.5	Function Provided by the M2UA Layer.....	8
1.6	Definition of the M2UA Boundaries.....	9
2.	Conventions.....	9
3.	Protocol Elements.....	9
3.1	Common Message Header.....	10
3.2	M2UA Message Header.....	11
3.3	M2UA Messages.....	11
4.	Procedures.....	20
4.1	Procedures to Support Service in Section 1.4.1.....	20
4.2	Procedures to Support Service in Section 1.4.2.....	21
4.3	Procedures to Support Service in Section 1.4.3.....	21
5.	Examples of MTP2 User Adaptation (M2UA) Procedures.....	26
5.1	Establishment of associations between SG and MGC.....	26
	examples	
5.2	MTP Level 2 / MTP Level 3 Boundary Examples.....	28
5.3	Layer Management Communication Examples.....	29
6.	Security.....	30
7.	IANA Considerations.....	31
8.	Acknowledgements.....	31
9.	References.....	32
10.	Author's Addresses.....	33

1. Introduction

1.1 Scope

There is a need for SCN signaling protocol delivery from an Signaling Gateway (SG) to a Media Gateway Controller (MGC) or IP Signaling Point (IPSP). The delivery mechanism should meet the following criteria:

- * Support for MTP Level 2 / MTP Level 3 interface boundary
- * Support for communication between Layer Management modules on SG and MGC
- * Support for management of active associations between the SG and MGC

In other words, the Signaling Gateway will transport MTP Level 3 messages to a Media Gateway Controller (MGC) or IP Signaling Point (IPSP). In the case of delivery from an SG to an IPSP, both the SG and IPSP function as traditional SS7 nodes using the IP network as a new type of SS7 link. This allows for full MTP Level 3 message handling and network management capabilities.

1.2 Terminology

MTP2-User - A protocol that normally uses the services of MTP Level 2 (i.e. MTP3).

Interface - For the purposes of this document, an interface is a SS7 signaling link.

Association - An association refers to a SCTP association. The association will provide the transport for the delivery of protocol data units for one or more interfaces.

Backhaul - Refers to the transport of signaling from the point of interface for the associated data stream (i.e., SG function in the MGU) back to the point of call processing (i.e., the MGCU), if this is not local [\[4\]](#).

Application Server (AS) - A logical entity serving a specific application instance. An example of an Application Server is a MGC handling the MTP Level 3 and call processing for SS7 links terminated by the Signaling Gateways. Practically speaking, an AS is modeled at the SG as an ordered list of one or more related Application Server Processes (e.g., primary, secondary, tertiary, ...).

Application Server Process (ASP) - A process instance of an Application Server. Examples of Application Server Processes are primary or backup MGC instances.

Application Server Process Path (ASP Path or just Path) - A Path to a

remote Application Server Process instance. A Path maps 1:1 to an SCTP association.

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

Signaling Link Terminal (SLT) - Refers to the means of performing all of the functions defined at MTP level 2 regardless of their implementation [2].

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

Layer Management - Layer Management is a nodal function in an SG or ASP that handles the inputs and outputs between the M2UA layer and a local management entity.

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

Stream - A stream refers to an SCTP stream.

1.3 Signaling Transport Architecture

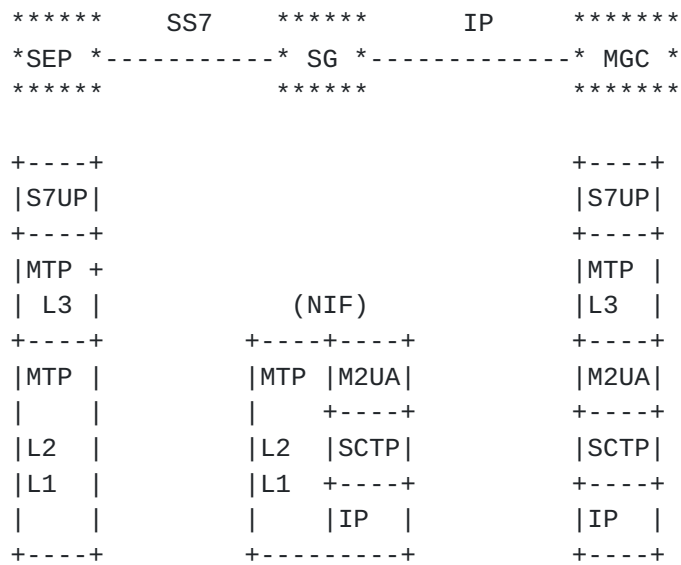
The framework architecture that has been defined for SCN signaling transport over IP [5] uses multiple components, including a signaling common transport protocol and an adaptation module to support the services expected by a particular SCN signaling protocol from its underlying protocol layer.

Within this framework architecture, this document defines a SCN adaptation module that is suitable for the transport of SS7 MTP2 User messages. The only SS7 MTP2 User is MTP3. The M2UA uses the services of the Simple Common Transport protocol [6] as the underlying reliable signaling common transport protocol.

In a Signaling Gateway, it is expected that the SS7 MTP2-User signaling is transmitted and received from the PSTN over a standard SS7 network interface, using the SS7 Message Transfer Part Level 1 and Level 2 [3,4] to provide reliable transport of the MTP3-User signaling messages to and from an SS7 Signaling End Point (SEP) or Signaling Transfer Point (STP). The SG then provides a functional inter-working of transport functions with the IP transport, in order to transfer the MTP2-User signaling messages to and from an Application Server Process where the peer MTP2-User protocol layer exists.

1.3.1 Example - SG to MGC

In a Signaling Gateway, it is expected that the SS7 signaling is received over a standard SS7 network termination, using the SS7 Message Transfer Part (MTP) to provide transport of SS7 signaling messages to and from an SS7 Signaling End Point (SEP) or SS7 Signaling Transfer Point (STP). In other words, the SG acts as a Signaling Link Terminal (SLT) [2]. The SG then provides interworking of transport functions with IP Signaling Transport, in order to transport the MTP3 signaling messages to the MGC where the peer MTP3 protocol layer exists, as shown below:



NIF - Nodal Interworking Function
 SEP - SS7 Signaling Endpoint
 IP - Internet Protocol
 SCTP - Simple Control Transmission Protocol
 (Refer to Reference [5])

Figure 1 M2UA in the SG to MGC Application

Note: STPs may be present in the SS7 path between the SEP and the SG.

1.3.2 Signaling Network Architecture

A Signaling Gateway will support the transport of MTP2-User signaling traffic received from the SS7 network to one or more distributed ASPs (e.g., MGCs). Clearly, the M2UA protocol description cannot in itself meet any performance and reliability requirements for such transport. A physical network architecture is required, with data on the availability and transfer performance of the physical nodes involved in any particular exchange of information. However, the M2UA protocol must be flexible enough allow its operation and management in a variety of physical configurations that will enable Network Operators to meet their performance and reliability requirements.

To meet the stringent SS7 signaling reliability and performance requirements for carrier grade networks, these Network Operators should ensure that there is no single point of failure provisioned in the end-to-end network architecture between an SS7 node and an IP ASP. Depending of course on the reliability of the SG and ASP functional elements, this can typically be met by the spreading links in a linkset across SGs, the provision of redundant QOS-bounded IP network paths for SCTP Associations between SCTP End Points, and redundant Hosts. The distribution of ASPs

within the available Hosts is also important. For a particular Application Server, the related ASPs should be distributed over at least two Hosts.

An example physical network architecture relevant to carrier-grade operation in the IP network domain is shown in Figure 2 below:

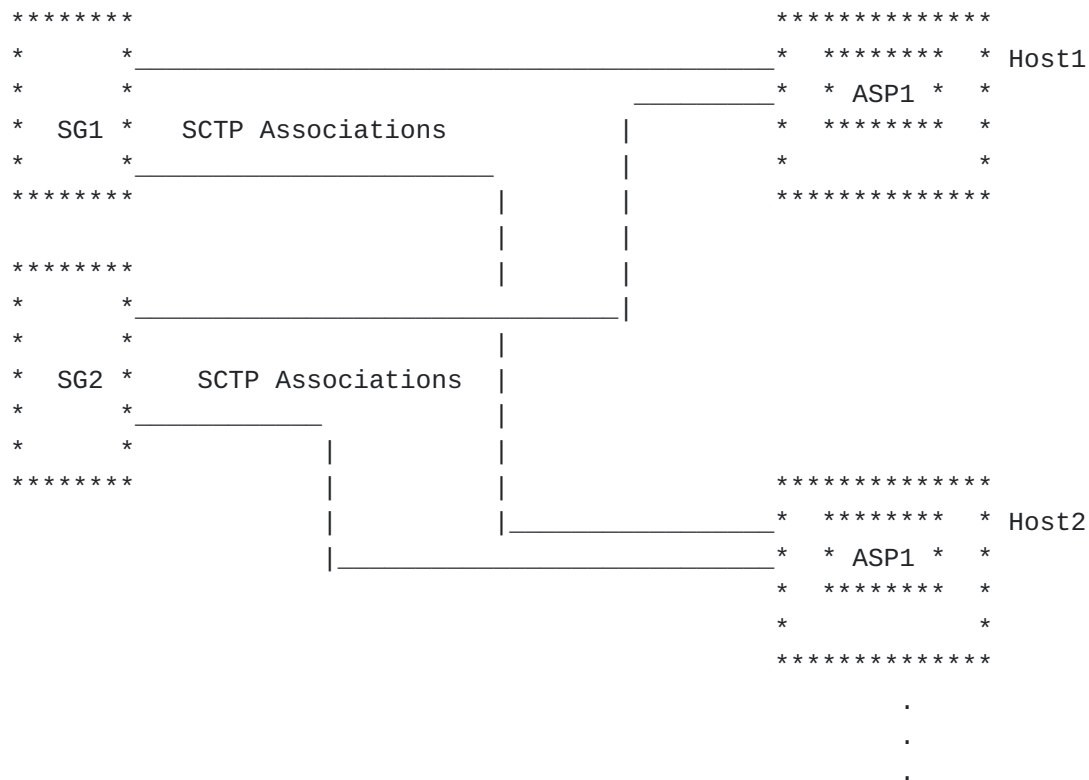


Figure 2 - Physical Model Example

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

1.3.4 ASP Fail-over Model and Terminology

The M2UA supports ASP fail-over functions in order to support a high availability of call and transaction processing capability. All MTP2-User messages incoming to an SG from the SS7 network are assigned to a unique Application Server, based on the Interface Identifier of the message.

The Application Server is in practical terms a list of all ASPs currently registered to process MTP2-User messages from certain Interface Identifiers. One or more ASPs in the list are normally active (i.e., handling traffic) while any others may be unavailable or inactive, to be possibly used in the event of failure or unavailability of the active

ASP(s).

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

To avoid a single point of failure, it is recommended that a minimum of two ASPs be in the list, resident in separate hosts and therefore available over different SCTP Associations. For example, in the network shown in Figure 1, all messages to DPC x could be sent to ASP1 in Host1 or ASP1 in Host2. The AS list at SG1 might look like this:

```
Interface Identifiers - Application Server #1
  ASP1/Host1 - State=Up, Active
  ASP1/Host2 - State=Up, Inactive
```

In this 1+1 redundancy case, ASP1 in Host1 would be sent any incoming message for the Interface Identifiers registered. ASP1 in Host2 would normally be brought to the active state upon failure of, or loss of connectivity to, ASP1/Host1. In this example, both ASPs are Up, meaning that the related SCTP association and far-end M2UA peer is ready.

The AS List at SG1 might also be set up in loadshare mode:

```
Interface Identifiers - Application Server #1
  ASP1/Host1 - State = Up, Active
  ASP1/Host2 - State = Up, Active
```

In this case, both the ASPs would be sent a portion of the traffic.

In the process of fail-over or fail-back, 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.

1.3.5 Client/Server Model

It is recommended that the SG take on the role of server while the ASP is the client. ASPs should initiate the SCTP association to the SG.

The SCTP (and UDP/TCP) Registered User Port Number Assignment for M2UA is 2904.

1.4 Services Provided by the M2UA Adaptation Layer

The SS7 MTP3/MTP2(MTP2-User) interface is retained at the termination point in the IP network, so that the M2UA protocol layer is required to provide the equivalent set of services to its users as provided by the MTP Level 2 to MTP Level 3.

This includes the following services:

1.4.1 Support for MTP Level 2 / MTP Level 3 interface boundary

Also provision is made for protocol elements that enable a seamless, or as seamless as possible, operation of the MTP2-User peers in the SS7 and IP domains. This includes

Data

Provides the ability to transport MTP2 User information (in this case, MTP Level 3 PDUs).

Link Establish

Provides the ability to request MTP Level 2 to bring SS7 links in-service.

Link Release

Provides the ability to request MTP Level 2 to take SS7 links out-of-service. Also, provides mechanism for MTP2 to autonomously indicate that SS7 link(s) have gone out-of-service.

Link State

Provides the ability to request state change or information on a per link basis. Some examples would be the forcing of Local Processor Outage or flushing buffers.

Link Status

Provides a means for asynchronous notification of link state changes to be reported to the upper layer (MTP Level 3). An example would be the reporting of remote processor outage event.

Data Retrieval

Provides a mechanism to perform SS7 link changeover procedure in the case of a SS7 link failure.

1.4.2 Support for communication between Layer Management modules on SG and MGC

It is envisioned that the M2UA layer needs to provide some messages that will facilitate communication between Layer Management modules on the SG and MGC.

To facilitate reporting of errors that arise because of backhauling MTP Level 3 scenario, the following primitive is defined:

M-ERROR

The M-ERROR message is used to indicate an error with a received M2UA message (e.g., interface identifier value is not known to the SG).

1.4.3 Support for management of active associations between SG and MGC

The M2UA layer on the SG keeps the state of various ASPs it is associated with. A set of primitives between M2UA layer and the Layer Management are defined below to help the Layer Management manage the association(s) between the SG and the MGC.

M-SCTP ESTABLISH

The M-SCTP ESTABLISH primitive is used to request, indicate and confirm the establishment of SCTP association to a peer M2UA node.

The M2UA layer may also need to inform the status of the SCTP association(s) to the Layer Management. This can be achieved using the following primitive.

M-SCTP STATUS

The M-SCTP STATUS primitive is used to request and indicate the status of underlying SCTP association(s).

The Layer Management may need to inform the M2UA layer of a user status (i.e., failure, active, etc.), so that messages can be exchanged between M2UA layer peers to stop traffic to the local M2UA user. This can be achieved using the following primitive.

M-ASP STATUS

The M-ASP STATUS primitive is used by the Layer Management to indicate the status of the local M2UA user to the M2UA layer.

[1.5](#) Functions Provided by the M2UA Layer

[1.5.1](#) Mapping

The M2UA layer must maintain a map of a Interface ID to a physical interface on the Signaling Gateway. A physical interface would be a [V.35 line](#), [T1 line/timeslot](#), [E1 line/timeslot](#), etc. The M2UA layer must also maintain a map of Interface Identifier to SCTP association and to the related stream within the association.

[1.5.2](#) Flow Control / Congestion

It is possible for the M2UA layer to be informed of IP network congestion by means of an implementation-dependent function (i.e. an indication from the SCTP). If the M2UA layer receives this indication, the action(s) taken are implementation dependent.

[1.5.3](#) SCTP Stream Management

SCTP allows user specified number of streams to be opened during the initialization. It is the responsibility of the M2UA layer to ensure proper management of these streams. SCTP streams provide a means for avoiding head of line blocking. For that reason, a stream should be used per SS7 signaling link terminated by the Signaling Gateway. The SS7 signaling link can be identified by the optional Interface Identifier in the M2UA specific message header (refer to [Section 2.2](#)).

[1.5.4](#) Seamless SS7 Network Management Interworking

If the SG loses the SCTP association to the MGC, it should follow MTP 2 processor outage procedures [[2](#)].

1.5.5 Active Association Control

At an SG, an Application Server list may contain active and inactive ASPs to support ASP loads-haring and fail-over procedures. When, for example, both a primary and a back-up ASP are available, M2UA peer protocol is required to control which ASP is currently active. The ordered list of ASPs within a logical Application Server is kept updated in the SG to reflect the active Application Server Process(es).

1.6 Definition of the M2UA Boundaries

1.6.1 Definition of the M2UA / MTP Level 3 boundary

DATA
ESTABLISH
RELEASE
STATE
STATUS
RETRIEVAL
DATA RETRIEVAL
DATA RETRIEVAL COMPLETE

1.6.2 Definition of the M2UA / MTP Level 2 boundary

DATA
ESTABLISH
RELEASE
STATE
STATUS
RETRIEVAL
DATA RETRIEVAL
DATA RETRIEVAL COMPLETE

1.6.3 Definition of the Lower Layer Boundary between M2UA and SCTP

The upper layer and layer management primitives provided by SCTP are provided in Reference [\[6\]](#) [Section 9](#).

1.6.4 Definition of Layer Management / M2UA Boundary

M-ERROR
M-SCTP ESTABLISH
M-SCTP STATUS
M-ASP STATUS

2.0 Conventions

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, NOT RECOMMENDED, MAY, and OPTIONAL, when they appear

in this document, are to be interpreted as described in [[RFC2119](#)].

[3.0](#) Protocol Elements

This section describes the format of various messages used in this protocol.

3.1 Common Message Header

The protocol messages for MTP2-User Adaptation require a message structure which contains a version, message type, message length, and message contents. This message header is common among all signaling protocol adaptation layers:

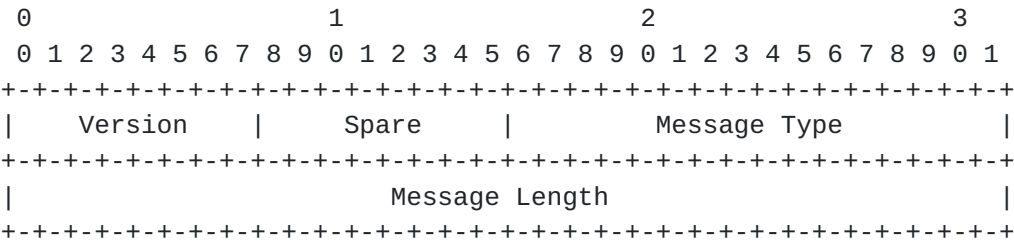


Figure 3 Common Message Header

All fields in an M2UA message MUST be transmitted in the network byte order, unless otherwise stated.

3.1.1 Version

The version field (vers) contains the version of the M2UA adaptation layer. The supported versions are:

Release 1.0 0x1

3.1.2 Message Type

The valid message types are defined in [Section 3.2.2](#) and the message contents are described in [Section 3.3](#). Each message can contain parameters.

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

MTP2 User Adaptation (MAUP) Messages

Data	0x0601
Establish Request	0x0602
Establish Confirm	0x0603
Release Request	0x0604
Release Confirm	0x0605
Release Indication	0x0606
State Request	0x0607
State Confirm	0x0608
State Indication	0x0609
Data Retrieval Request	0x060a
Data Retrieval Confirm	0x060b

Data Retrieval Indication	0x060c
Data Retrieval Complete Indication	0x060d

Application Server Process Maintenance (ASPM) Messages

ASP Up	0x0301
ASP Down	0x0302
Heartbeat	0x0303
ASP Up Ack	0x0304
ASP Down Ack	0x0305
ASP Active	0x0401
ASP Inactive	0x0402
ASP Active	0x0403
ASP Inactive	0x0404

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 should NEVER pad with more than 3 bytes. The receiver MUST ignore the padding bytes.

3.2 M2UA Message Header

In addition to the common message header, there will be a M2UA specific message header. The M2UA specific message header will immediately follow the common message header, but will only be used with MAUP messages.

This message header will contain the Interface Identifier. The Interface Identifier identifies the physical interface at the SG for which the signaling messages are sent/received. The format of the Interface Identifier parameter is an integer, the values of which are assigned according to network operator policy. The values used are of local significance only, coordinated between the SG and ASP.

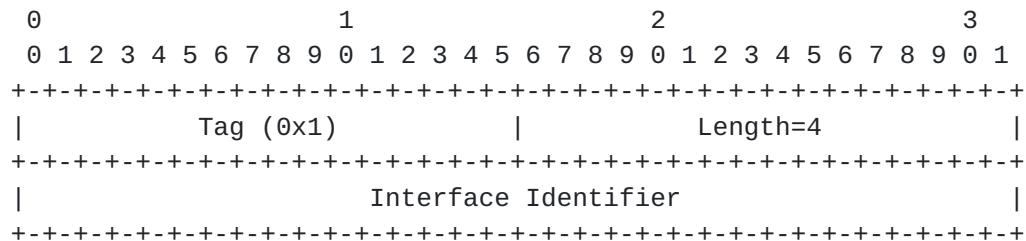


Figure 4 M2UA Message Header

The Tag value for Interface Identifier is 0x1. The length is always set to a value of 8.

3.3 M2UA Messages

The following section defines the messages and parameter contents. The M2UA messages will use the common message header (Figure 3) and the M2UA message header (Figure 4).

3.3.3.1 MTP2 User Adaptation Messages

3.3.1.1 Data

The Data message contains an SS7 MTP2-User Protocol Data Unit (PDU). The Data message contains the protocol data.

RELEASE_SUERM	0x7	Release due to failure reported by SUERM
RELEASE_IAC	0x8	Release due to initial alignment failed
RELEASE_OTHER	0x9	Other reason SS7 link out-of-service

3.3.1.4 State (Request, Confirm)

The State Request message can be sent from a MGC to cause an action on a particular SS7 link supported by the Signaling Gateway. The gateway sends a State Confirm to the MGC if the action has been successfully completed. The State Confirm reflects that state value received in the State Request 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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     State                             |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

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

Define	Value	Description
STATUS_LPO_SET	0x0	Request local processor outage
STATUS_LPO_CLEAR	0x1	Request local processor outage recovered
STATUS_EMER_SET	0x2	Request emergency alignment procedure
STATUS_EMER_CLEAR	0x3	Request normal alignment (cancel emergency) procedure
STATUS_FLUSH_BUFFERS	0x4	Flush transmit and retransmit buffers
STATUS_CONTINUE	0x5	Continue

[3.3.1.5](#) State Indication

The MTP2 State Indication message can be sent from a gateway to an ASP to indicate a condition on a link.

```

      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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     State                             |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

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

Define	Value	Description
EVENT_ENTER_LPO	0x0	Entered local processor outage
EVENT_EXIT_LPO	0x1	Exited local processor outage
EVENT_ENTER_CONG	0x2	Entered a congested state
EVENT_EXIT_CONG	0x3	Exited a congested state
EVENT_PHYS_UP	0x4	Physical interface up
EVENT_PHYS_DOWN	0x5	Physical interface down
EVENT_PROTOCOL_ERR	0x6	Protocol error occurred
EVENT_REM_ENTER_CONG	0xc	Remote entered congestion
EVENT_REM_EXIT_CONG	0xd	Remote exited congestion
EVENT_REM_ENTER_PO	0xe	Remote entered processor outage
EVENT_REM_EXIT_PO	0xf	Remote exited processor outage

[3.3.1.6](#) Retrieval (Request, Confirm)

The MTP2 Retrieval Request message is used during the MTP Level 3 changeover procedure to request the BSN, to retrieve PDUs from the retransmit queue or to flush PDUs from the retransmit queue.

```

      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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     Action                                     |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                                     fsn_bsn                                    |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

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

Define	Value	Description
ACTION_RTRV_BSN	0x1	Retrieve the backward sequence number
ACTION_RTRV_MSGS	0x2	Retrieve the PDUs from the retransmit queue
ACTION_DROP_MSGS	0x3	Drop the PDUs in the retransmit queue

In the Retrieval Request message, the fsn_bsn field contains the FSN of the far end if the action is ACTION_RTRV_MSGS.

When the Signaling Gateway sends a Retrieval Confirm to this request, it echos the action and puts the BSN in the fsn_bsn field if the action was ACTION_RTRV_BSN. If there is a failure in retrieving the BSN, the fsn_bsn should contain a -1 (0xffffffff).

[3.3.1.7](#) Retrieval Indication

The Retrieval Indication message is sent by the Signaling Gateway with a PDU from the retransmit queue. The Retrieval Indication message does not contain the Action or fsn_bsn fields, just a PDU from the retransmit queue.

```

      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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
|                                     PDU from retransmit queue
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

[3.3.1.8](#) Retrieval Complete Indication

The MTP2 Retrieval Complete Indication message is exactly the same as the MTP2 Retrieval Indication message except that it also indicates that it contains the last PDU from the retransmit queue.

[3.3.2](#) Application Server Process Maintenance (ASPM) Messages

The ASPM messages will only use the common message header.

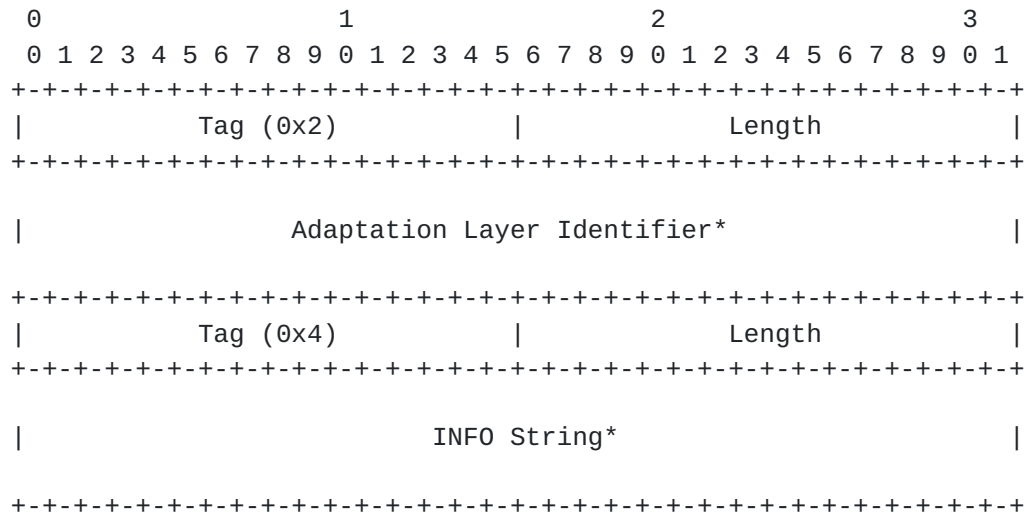
3.3.2.1 ASP UP (ASPUP)

The ASP UP (ASPUP) message is used to indicate to a remote M2UA peer that the Adaptation layer is ready to receive traffic or maintenance messages.

The ASPUP message contains the following parameters:

Adaptation Layer Identifier (optional)
 Protocol Identifier (optional)
 INFO String (optional)

The format for ASPUP Message parameters is as follows:



The optional INFO String parameter can carry any meaningful 8-bit ASCII character string along with the message. Length of the INFO String parameter is from 0 to 255 characters. No procedures are presently identified for its use but the INFO String may be used for debugging purposes.

The optional Adaptation Layer Identifier (ALI) is a string that identifies the adaptation layer. This string must be set to "M2UA" which results in a length of 8. The ALI would normally only be used in the initial ASP Up message across a new SCTP association to ensure both peers are assuming the same adaptation layer protocol.

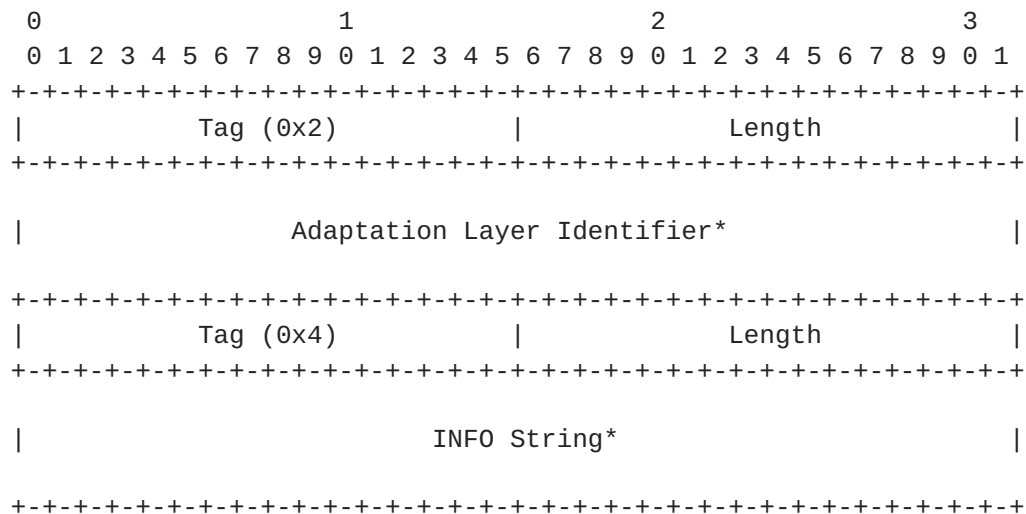
3.3.3.2 ASP Up Ack

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

The ASPUP Ack message contains the following parameters:

Adaptation Layer Identifier (optional)
INFO String (optional)

The format for ASPUP Ack Message parameters is as follows:



The format and description of the optional Info String parameter is the same as for the ASP UP message (See [Section 3.3.3.1](#).)

The format and description of the optional Adaptation Layer Identifier (ALI) parameter is the same as for the ASP UP message (See [Section 3.3.3.1](#)).

3.3.3.3 ASP Down (ASPDN)

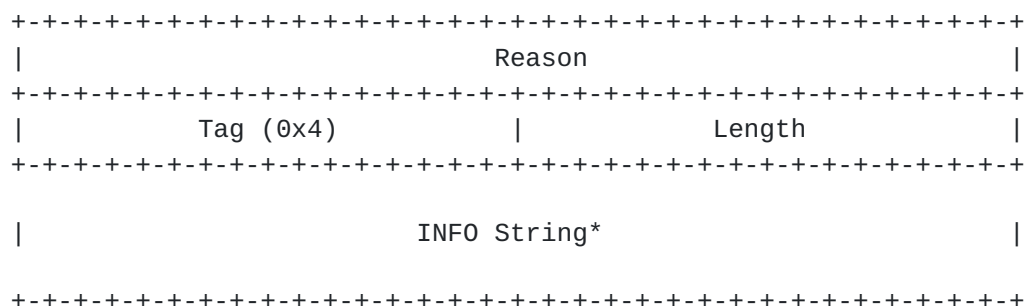
The ASP Down (ASPDN) message is used to indicate to a remote IUA peer that the adaptation layer is not ready to receive traffic or maintenance messages.

The ASPDN message contains the following parameters

Reason
INFO String (Optional)

The format for the ASPDN message parameters is as follows:





The format and description of the optional Info String parameter is the same as for the ASP Up message (See [Section 3.3.2.1.](#))

The Reason parameter indicates the reason that the remote M2UA adaptation layer is unavailable. The valid values for Reason are shown in the following table.

Value	Description
0x1	Management Inhibit

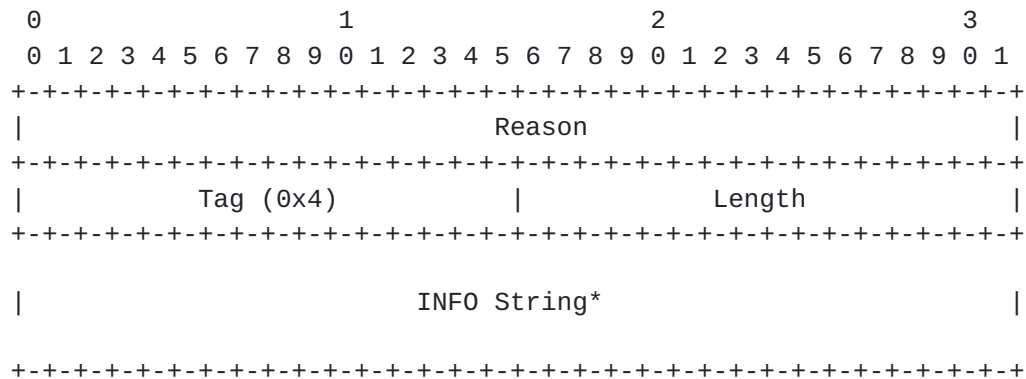
3.4.4 ASP Down Ack

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

The ASP Down Ack message contains the following parameters:

Reason
INFO String (Optional)

The format for the ASPDN Ack message parameters is as follows:



The format and description of the optional Info String parameter is the same as for the ASP UP message (See [Section 3.3.3.1.](#))

The format of the Reason parameter is the same as for the ASP-Down message (See [Section 3.3.3.3.](#)).

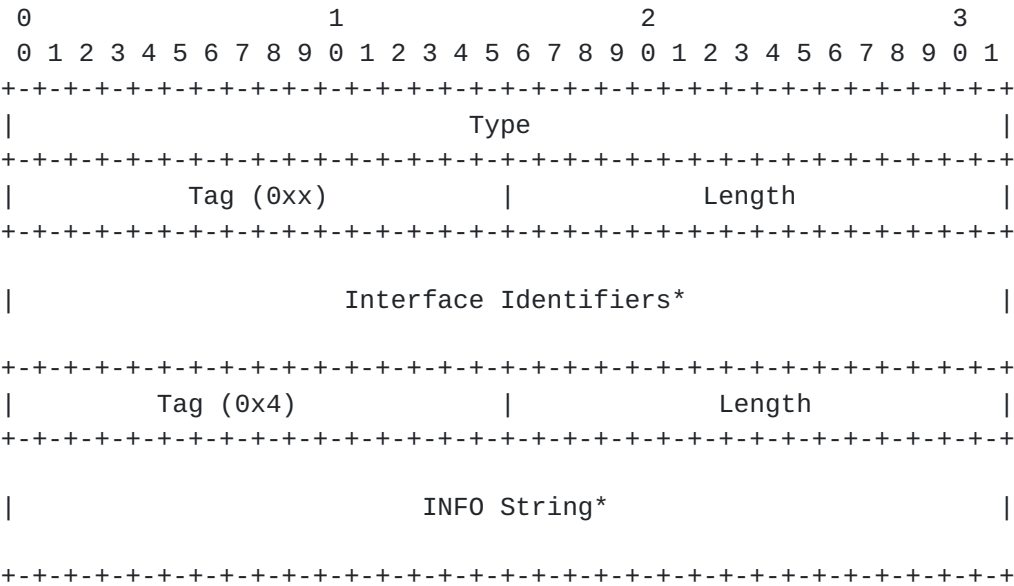
3.3.3.5 ASP Active (ASPAC)

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

The ASPAC message contains the following parameters

- Type
- Interface Identifier (Optional)
- INFO String (Optional)

The format for the ASPAC message is as follows:



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

Value	Description
0x1	Over-ride
0x2	Load-share

Within a particular Interface Identifier, only one Type can be used. The Over-ride value indicates that the ASP is operating in Over-ride mode, where the ASP takes over all traffic in an Application Server (i.e., primary/back-up operation), over-riding any currently active ASPs in the AS. In Load-share mode, the ASP will share in the traffic distribution with any other currently active ASPs.

The optional Interface Identifiers parameter contains a list of Interface Identifier integers indexing the Application Server traffic that the sending ASP is configured/registered to receive. There is one-to-one relationship between an Interface Identifier and an AS Name.

An SG that receives an ASPAC with an incorrect type for a particular Interface Identifier will respond with an Error Message.

The format and description of the optional Info String parameter is the same as for the ASP UP message (See [Section 3.3.3.1.](#))

A node that receives an ASPAC with an incorrect Type for a particular Interface Identifier will respond with an Error Message (Cause: Invalid Traffic Handling Mode).

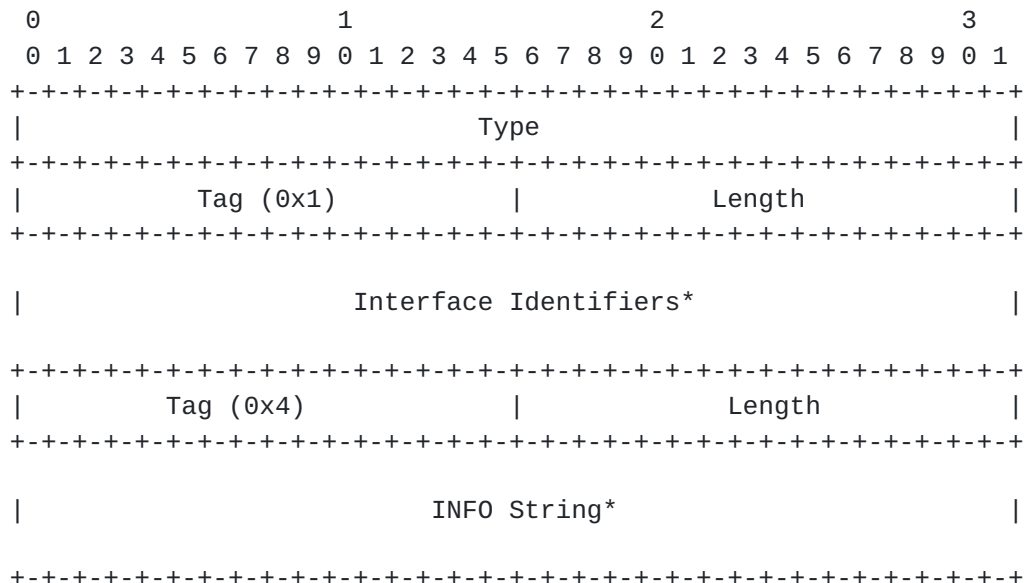
[3.3.3.6](#) ASP Active Ack

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

The ASPAC Ack message contains the following parameters:

Type
Interface Identifier (Optional)
INFO String (Optional)

The format for the ASPAC Ack message is as follows:



The format and description of the optional Info String parameter is the

same as for the ASP UP message (See [Section 3.3.3.1.](#))

The format of the Type and Interface Identifier parameters is the same as for the ASP Active message (See [Section 3.3.3.5](#)).

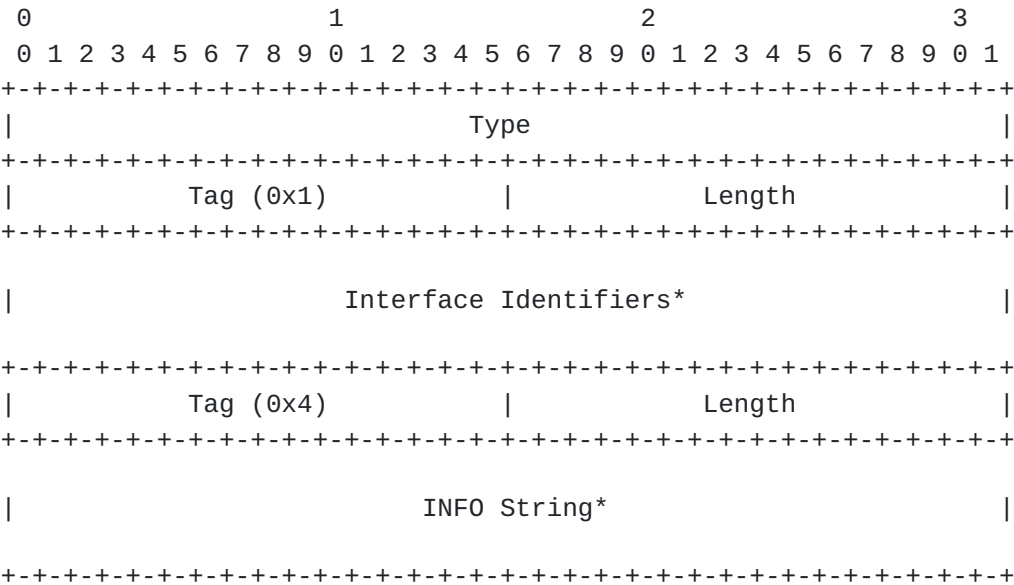
[3.3.3.7](#) ASP Inactive (ASPIA)

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

The ASPIA message contains the following parameters

- Type
- Interface Identifiers (Optional)
- INFO String (Optional)

The format for the ASPIA message parameters is as follows:



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

Value	Description
0x1	Over-ride
0x2	Load-share

The format and description of the optional Interface Identifiers and Info String parameters is the same as for the ASP Active message (See [Section 3.3.3.3.](#))

The optional Interface Identifiers parameter contains a list of Interface Identifier integers indexing the Application Server traffic

that the sending ASP is configured/registered to receive, but does not want to receive at this time.

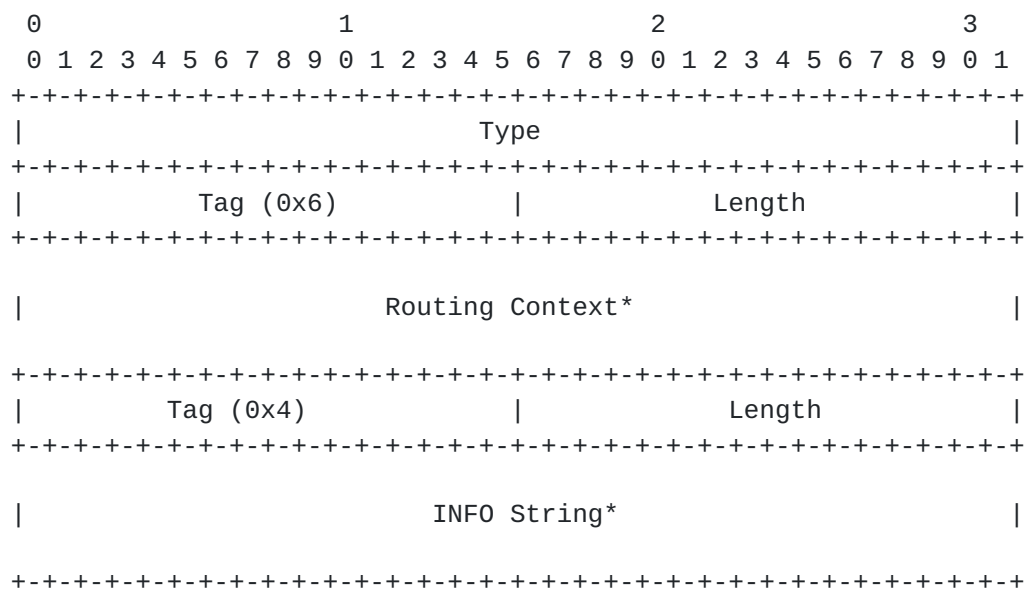
3.3.3.8 ASP Inactive Ack

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

The ASPIA Ack message contains the following parameters:

```
Type
Routing Context (Optional)
INFO String (Optional)
```

The format for the ASPIA Ack message is as follows:



The format and description of the optional Info String parameter is the same as for the ASP UP message (See [Section 3.3.3.1.](#))

The format of the Type and Routing Context parameters is the same as for the ASP-Inctive message (See [Section 3.3.3.7](#)).

3.4.9 Heartbeat (BEAT)

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

The BEAT message contains no parameters.

3.3.3.3 Layer Management (MGMT) Messages

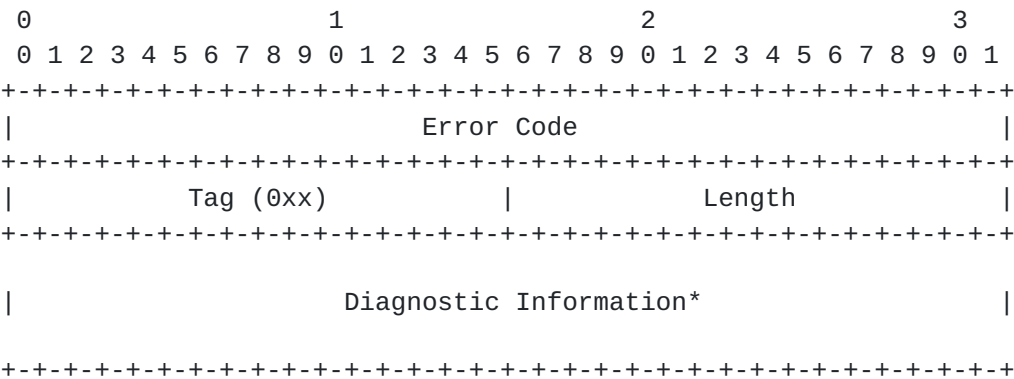
3.3.3.1 Error (ERR)

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.

The ERR message contains the following parameters:

- Error Code
- Diagnostic Information (optional)

The format for the ERR message is as follows:



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

- | | |
|-------------------------------------|-----|
| Invalid Version | 0x1 |
| Invalid Interface Identifier | 0x2 |
| Invalid Adaptation Layer Identifier | 0x3 |
| Invalid Message Type | 0x4 |
| Invalid Traffic Handling Mode | 0x5 |
| Unexpected Message | 0x6 |
| Protocol Error | 0x7 |
| Invalid Stream Identifier | 0x8 |

The optional Diagnostic information can be any information german to the error condition, to assist in identification of the error condition. In the case of an Invalid Version Error Code the Diagnostic information includes the supported Version parameter. In the other cases, the Diagnostic information may be the first 40 bytes of the offending message.

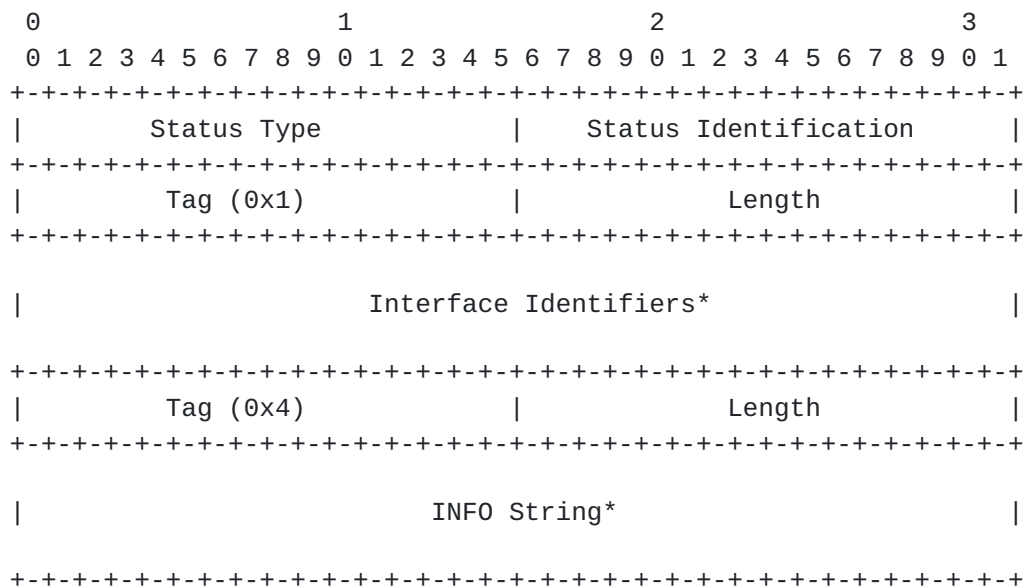
3.3.3.2 Notify (NTFY)

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

The NTFY message contains the following parameters:

Status Type
 Status Identification
 Interface Identifiers (Optional)
 INFO String (Optional)

The format for the NTFY message is as follows:



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

Value	Description
0x1	Application Server state change (AS_State_Change)
0x2	Other

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:

Value	Description
0x1	Application Server Down (AS_Down)
0x2	Application Server Up (AS_Up)
0x3	Application Server Active (AS_Active)
0x4	Application Server Pending (AS_Pending)

0x5 Alternate ASP Active

These notifications are sent from an SG 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:

Value	Description
0x1	Insufficient ASP resources active in AS

This notification is not based on the SG reporting the state change of an ASP or AS. For the value defined the SG is indicating to an ASP(s) in the AS that another ASP is required in order to handle the load of the AS.

The format and description of the optional Interface Identifiers and Info String parameters is the same as for the ASP Active message (See [Section 3.3.3.3.](#))

4.0 Procedures

The M2UA layers needs to respond to various primitives it receives from other layers as well as messages it receives from the peer-to-peer messages. This section describes various procedures involved in response to these events.

4.1 Procedures to Support Service in [Section 1.4.1](#)

These procedures achieve the M2UA layer's "Transport of MTP Level 2 / MTP Level 3 boundary" service.

4.1.1 MTP Level 2 / MTP Level 3 Boundary Procedures

On receiving a primitive from the local upper layer, the M2UA layer will send the corresponding MAUP message (see [Section 2](#)) to its peer. The M2UA layer must fill in various fields of the common and specific headers correctly. In addition the message needs to be sent on the SCTP stream that corresponds to the SS7 link.

4.1.2 MAUP Message Procedures

On receiving MAUP messages from a peer M2UA layer, the M2UA layer on an SG or MGC needs to invoke the corresponding layer primitives to the local MTP Level 2 or MTP Level 3 layer.

4.2 Procedures to Support Service in Section 1.4.2

These procedures achieve the M2UA layer's "Support for Communication between Layer Managements" service.

4.2.1 Layer Management Primitives Procedure

On receiving these primitives from the local layer, the M2UA layer will send the corresponding MGMT message (Error) to its peer. The M2UA layer must fill in the various fields of the common and specific headers correctly.

4.2.2 MGMT message procedures

Upon receipt of MGMT messages the M2UA layer must invoke the corresponding Layer Management primitives (M-ERROR) to the local layer management.

4.3 Procedures to Support Service in Section 1.4.3

These procedures achieve the M2UA layer's "Support for management of active associations between SG and MGC" service.

4.3.1 State Maintenance

The M2UA layer on the SG maintains the state of each AS, in each Application Server that it is configured to receive traffic.

4.3.1.1 ASP States

The state of the each ASP, in each AS that it is configured, is maintained in the IUA layer on the SG. The state of an ASP changes due to events. The events include

- * Reception of messages from peer IUA layer at that ASP
- * Reception of some messages from the peer IUA layer at other ASPs in the AS
- * Reception of indications from SCTP layer
- * Switch-over Time triggers

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

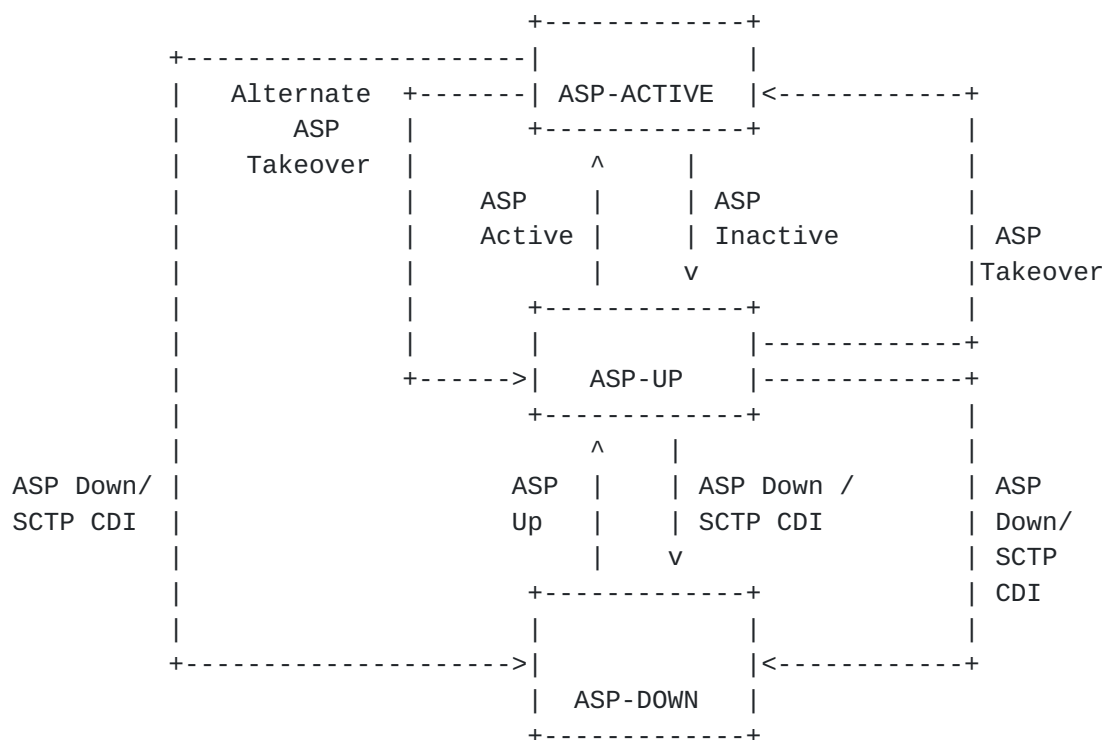
ASP-DOWN Application Server Process is unavailable and/or the SCTP association is down. Initially all ASPs will be in this state.

ASP-UP The remote IUA peer at the ASP is available (and the SCTP association is up) but application traffic is stopped.

ASP-ACTIVE The remote IUA peer at the ASP is available and

application traffic is active.

Figure 4 ASP State Transition Diagram



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

Ts Switch-over Time Triggers. This timer is configurable by the Operator on a per AS basis. The default value of this timer should be three seconds.

4.3.1.2 AS States

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

The state of an AS changes due to events. These events include the following:

- * ASP state transitions
- * Recovery timer triggers

The possible states of an AS are the following:

AS-DOWN The Application Server is unavailable. This state implies that all related ASPs are in the ASP-DOWN state for this AS. Initially the AS will be in this state.

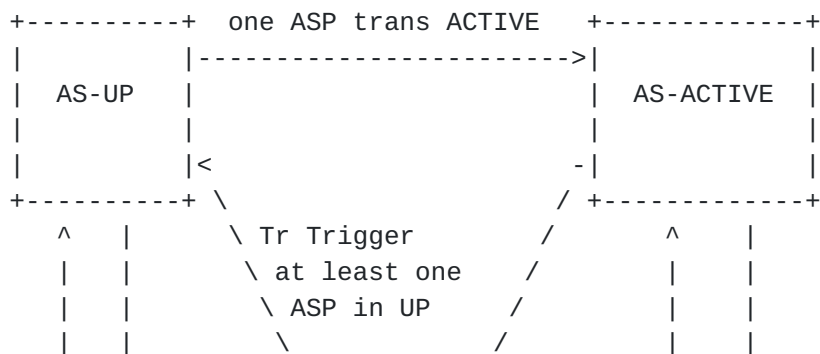
AS-UP The Application Server is available but no application traffic is active (i.e., one or more related ASPs are in the ASP-UP state, but none in the ASP-Active state).

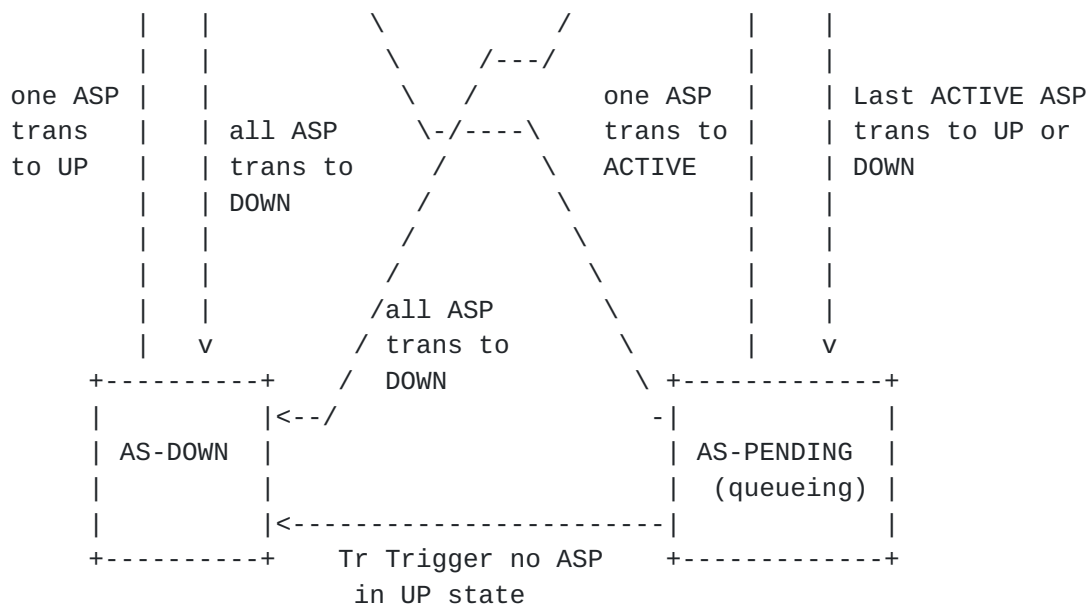
AS-ACTIVE The Application Server is available and application traffic is active. This state implies that one ASP is in the ASP-ACTIVE state.

AS-PENDING An active ASP has transitioned from active to inactive or down and it was the last remaining active ASP in the AS. A recovery timer $T(r)$ will be started and all incoming SCN messages will be queued by the SG. If an ASP becomes active before $T(r)$ expires, the AS will move to AS-ACTIVE state and all the queued messages will be sent to the active ASP.

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

Figure 5 AS State Transition Diagram





Tr = Recovery Timer

4.3.2 ASPM procedures for primitives

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

As the ASP is responsible for initiating the setup of an SCTP association to an SG, the IUA layer at an ASP receives an M-SCTP ESTABLISH request primitive from the Layer Management, the IUA layer will try to establish an SCTP association with the remote IUA peer at an SG. Upon reception of an eventual SCTP-Communication Up confirm primitive from the SCTP, the IUA layer will invoke the primitive M-SCTP ESTABLISH confirm to the Layer Management.

At the SG, the IUA layer will receive an SCTP Communication Up indication primitive from the SCTP. The IUA layer will then invoke the primitive M-SCTP ESTABLISH indication to the Layer Management.

Once the SCTP association is established and assuming that the local IUA-User is ready, the local ASP IUA Application Server Process Maintenance (ASPM) function will initiate the ASPM procedures, using the ASP-Up/-Down/-Active/-Inactive messages to convey the ASP-state to the SG - see [Section 4.3.3](#).

The Layer Management and the IUA layer on SG can communicate the status of the application server using the M-AS STATUS primitives. The Layer Managements and the IUA layers on both the SG and ASP can communicate the status of an SCTP association using the M-SCTP STATUS primitives.

If the Layer Management on SG or ASP wants to bring down an SCTP association for management reasons, they would send M-SCTP RELEASE request primitive to the local IUA layer. The IUA layer would release the SCTP association and upon receiving the SCTP Communication Down indication from the underlying SCTP layer, it would inform the local Layer Management using M-SCTP RELEASE confirm primitive.

If the IUA layer receives an SCTP-Communication Down indication from the underlying SCTP layer, it will inform the Layer Management by invoking the M-SCTP RELEASE indication primitive. The state of the ASP will be moved to "Down" at both the SG and ASP.

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

4.3.3 ASPM procedures for peer-to-peer messages

All ASPM messages are sent on a sequenced stream to ensure ordering. SCTP stream 0 is used.

4.3.3.2 ASP-Up

After an ASP has successfully established an SCTP association to an SG, the SG waits for the ASP to send an ASP-Up message, indicating that the ASP IUA peer is available. The ASP is always the initiator of the ASP-Up exchange.

When an ASP-Up message is received at an SG and internally the ASP is not considered locked-out for local management reasons, the SG marks the remote ASP as Up. The SG responds with an ASP-Up Ack message in acknowledgement. The SG sends an-UP Ack message in response to a received ASP-Up message even if the ASP is already marked as "Up" at the SG.

If for any local reason the SG cannot respond with an ASP-Up, the SG responds to a ASP-Up with a Notify (ASP-Down) message.

At the ASP, the ASP-Up Ack message received from the SG is not acknowledged by the ASP. If the ASP does not receive a response from the SG, or an ASP-Down is received, the ASP may resend ASP-Up messages every 2 seconds until it receives a Notify (ASP-Up) message from the SG. The ASP may decide to reduce the frequency (say to every 5 seconds) if an ASP-Up Ack is not received after a few tries.

The ASP must wait for the ASP-Up Ack message from the SG before sending any ASP traffic control messages (ASPAC or ASPIA) or Data messages or it will risk message loss. If the SG receives Data messages before an ASP Up is received, the SG should discard.

4.3.3.2 ASP-Down

The ASP will send an ASP-Down to an SG when the ASP is to be removed from the list of ASPs in all Application Servers that it is a member.

The SG marks the ASP as "Down" and returns an ASP-Down Ack message to the ASP if one of the following events occur:

- an ASP-Down message is received from the ASP,
- another ASPM message is received from the ASP and the SG has locked out the ASP for management reasons.

The SG sends an ASP-Down Ack message in response to a received ASP-Down message from the ASP even if the ASP is already marked as "Down" at the SG.

If the ASP does not receive a response from the SG, the ASP may send ASP-Down messages every 2 seconds until it receives an ASP-Down Ack message from the SG or the SCTP association goes down. The ASP may decide to reduce the frequency (say to every 5 seconds) if an ASP-Down Ack is not received after a few tries.

4.3.3.3 M2UA Version Control

If a ASP-Up message with an unsupported version is received, the receiving end responds with an Error message, indicating the version the receiving node supports.

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

4.3.3.4 ASP-Active

Any time after the ASP has received a ASP-Up Ack from the SG, the ASP sends an ASP-Active (ASPAC) to the SG indicating that the ASP is ready to start processing traffic. In the case where an ASP is configured/-registered to process the traffic for more than one Application Server across an SCTP association, the ASPAC contains one or more Interface Identifiers to indicate for which Application Servers the ASPAC applies.

When an ASP Active (ASPAC) message is received, the SG responds to the ASP with a ASPAC Ack message acknowledging that the ASPAC was received and starts sending traffic for the associated Application Server(s) to that ASP.

There are two modes of Application Server traffic handling in the SG IUA - Over-ride and Load-balancing. The Type parameter in the ASPAC message indicates the mode used in a particular Application Server. If the SG determines that the mode indicates in an ASPAC is incompatible with the traffic handling mode currently used in the AS, the SG responds with an Error message indicating Invalid Traffic Handling Mode.

In the case of an Over-ride mode AS, reception of an ASPAC message at an SG causes the redirection of all traffic for the AS to the ASP that sent the ASPAC. The SG responds to the ASPAC with an ASP-Active Ack message to the ASP. Any previously active ASP in the AS is now considered Inactive and will no longer receive traffic from the SG within the AS. The SG sends a Notify (Alternate ASP-Active) to the previously active ASP in the AS, after stopping all traffic to that ASP.

In the case of a load-share mode AS, reception of an ASPAC message at an SG causes the direction of traffic to the ASP sending the ASPAC, in addition to all the other ASPs that are currently active in the AS. The algorithm at the SG for loadsharing traffic within an AS to all the active ASPs is application and network dependent. The algorithm could, for example be round-robin or based on information in the Data message, such as Interface ID, depending on the requirements of the application and the call state handling assumptions of the collection of ASPs in the AS. The SG responds to the ASPAC with a ASP-Active Ack message to the ASP.

4.3.3.5 ASP Inactive

When an ASP wishes to withdraw from receiving traffic within an AS, the ASP sends an ASP Inactive (ASPIA) to the SG. In the case where an ASP is configured/registered to process the traffic for more than one Application Server across an SCTP association, the ASPIA contains one or more Interface Ids to indicate for which Application Servers the ASPIA applies.

There are two modes of Application Server traffic handling in the SG IUA when withdrawing an ASP from service - Over-ride and Load-balancing. The Type parameter in the ASPIA message indicates the mode used in a particular Application Server. If the SG determines that the mode indicates in an ASPAC is incompatible with the traffic handling mode currently used in the AS, the SG responds with an Error message indicating Invalid Traffic Handling Mode.

In the case of an Over-ride mode AS, where normally another ASP has already taken over the traffic within the AS with an Over-ride ASPAC, the ASP which sends the ASPIA is already considered by the SG to be "Inactive" (i.e., in the "Up" state). An ASPIA 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 SG moves the ASP to the "Up" state and the AS traffic is re-allocated across the remaining "active" ASPs per the load-sharing algorithm currently used within the AS. AnASPIA Ack message is sent to the ASP after all traffic is halted to the ASP.

If no other ASPs are Active in the Application Server, the SG either discards all incoming messages for the AS or starts buffering the incoming messages for T(r)seconds, after which messages will be discarded. T(r) is configurable by the network operator. If the SG receives an ASPAC from an ASP in the AS before expiry of T(r), the buffered traffic is directed to the ASP and the timer is cancelled.

4.3.3.5 Notify

In the case where a Notify (AS-Up) message is sent by an SG that now has no ASPs active to service the traffic, the Notify does not force the ASP(s) receiving the message to become active. The ASPs remain in control of what (and when) action is taken.

4.3.3.6 Heartbeat

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 the SCTP).

Once the ASP sends an ASP-Up message to the SG, the ASP sends Beat messages periodically, subject to a provisionable timer $T(\text{beat})$. The SG M3UA, upon receiving a BEAT message from the ASP, responds with a BEAT message. If no BEAT message (or any other M3UA message), is received from the ASP within the timer $2 \cdot T(\text{beat})$, the ASP will consider the remote M3UA as 'Down'.

At the ASP, if no BEAT message (or any other M3UA message) is received from the SG within $2 \cdot T(\text{beat})$, the SG is considered unavailable. Transmission of BEAT messages is stopped and ASP-Up procedures are used to re-establish communication with the SG M3UA peer.

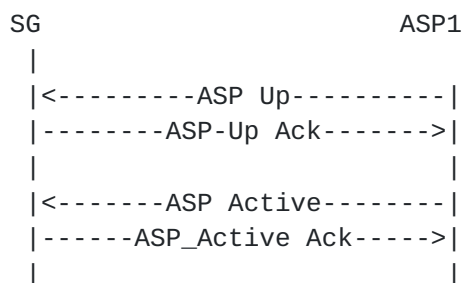
Note: Heartbeat related events are not shown in Figure 4 "ASP state transition diagram".

5.0 Examples of MTP2 User Adaptation (M2UA) Procedures

5.1 Establishment of associations between SG and MGC examples

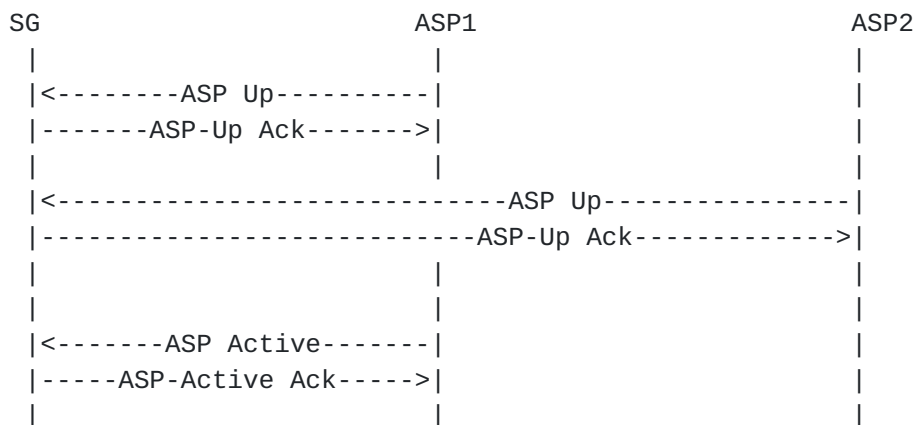
5.1.1 Single ASP in an Application Server (01+00 sparing)

This scenario shows the example M2UA message flows for the establishment of traffic between an SG and an ASP, where only one ASP is configured within an AS (no backup). It is assumed that the SCTP association is already set-up.



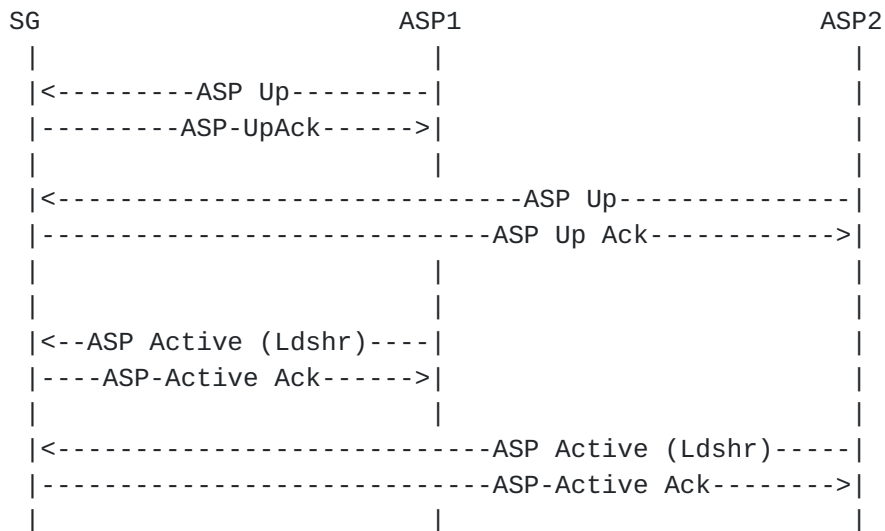
5.1.2 Two ASPs in Application Server (1+1 sparing)

This scenario shows the example M2UA message flows for the establishment of traffic between an SG and two ASPs in the same Application Server, where ASP1 is configured to be "active" and ASP2 a "standby" in the event of communication failure or the withdrawal from service of ASP1. ASP2 may act as a hot, warm, or cold standby 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 are Over-ride or Load-share mode although typically this example would use an Over-ride mode.



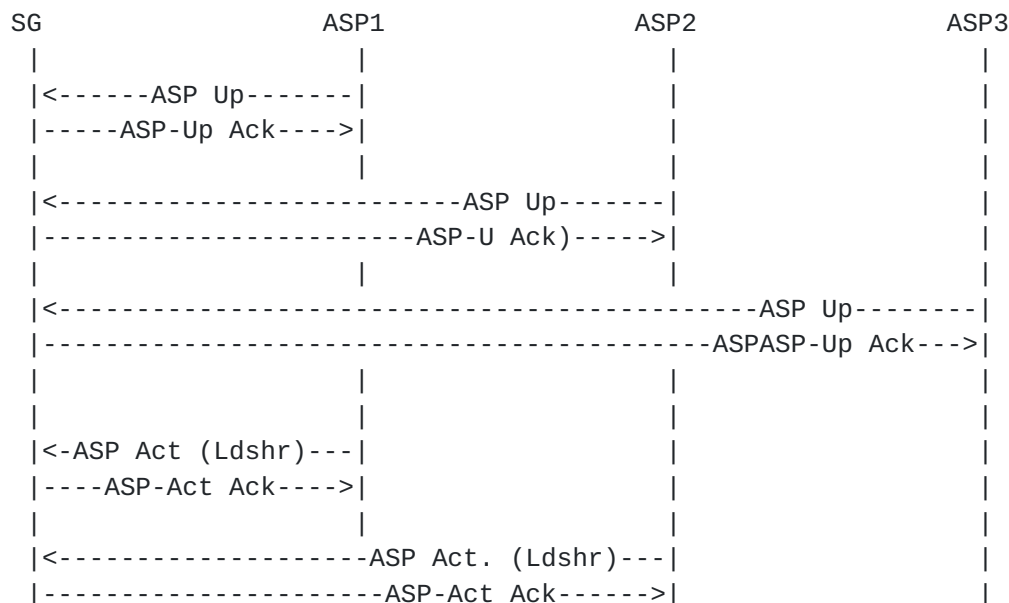
5.1.3 Two ASPs in an Application Server (1+1 sparing, load-sharing case)

This scenario shows a similar case to [Section 5.1.2](#) but where the two ASPs are brought to "active" and loadshare the traffic load. In this case, one ASP is sufficient to handle the total traffic load.



5.1.4 Three ASPs in an Application Server (n+1 sparing, load-sharing case)

This scenario shows the example M2UA message flows for the establishment of traffic between an SG and three ASPs in the same Application Server, where two of the ASPs are brought to "active" and share the load. In this case, a minimum of two ASPs are required to handle the total traffic load (2+1 sparing).



|

|

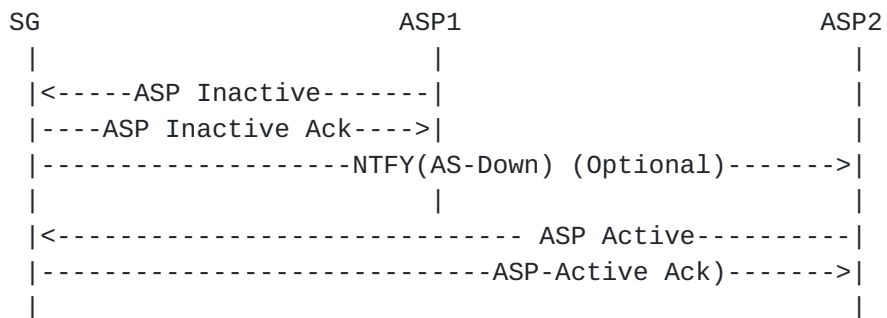
|

|

5.2 ASP Traffic Fail-over Examples

5.2.1 (1+1 Sparing, withdrawal of ASP, Back-up Over-ride)

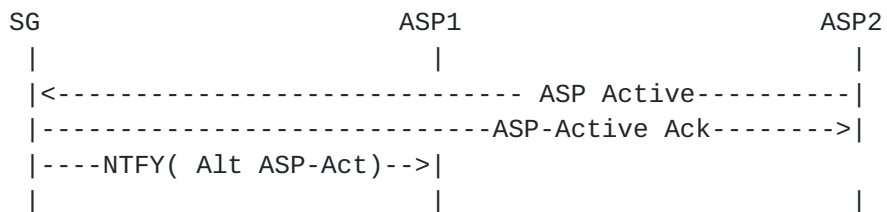
Following on from the example in [Section 5.1.2](#), and ASP withdraws from service:



Note: If the SG detects loss of the M2UA peer (M2UA heartbeat loss or detection of SCTP failure), the initial SG-ASP1 ASP Inactive message exchange would not occur.

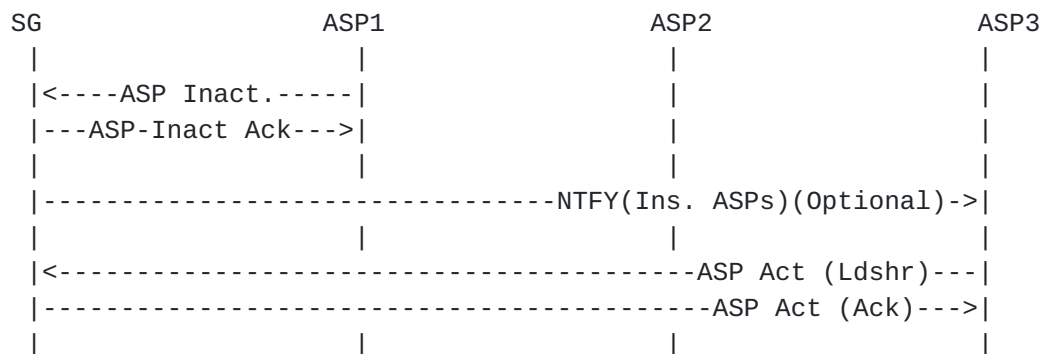
5.2.2 (1+1 Sparing, Back-up Over-ride)

Following on from the example in [Section 5.1.2](#), and ASP2 wishes to over-ride ASP1 and take over the traffic:



5.2.3 (n+k Sparing, Load-sharing case, withdrawal of ASP)

Following on from the example in [Section 5.1.4](#), and ASP1 withdraws from service:



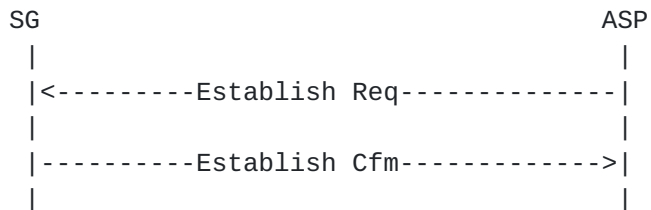
The Notify message to ASP3 is optional, as well as the ASP-Active from ASP3. The optional Notify can only occur if the SG maintains knowledge of the minimum ASP resources required - for example if the SG knows that $\hat{n} + k \leq \hat{n}_2 + 1$ for a loadshare AS and \hat{n} currently equals \hat{n}_1 .

Note: If the SG detects loss of the ASP1 M2UA peer (M2UA heartbeat loss or detection of SCTP failure), the first SG-ASP1 ASP Inactive message exchange would not occur.

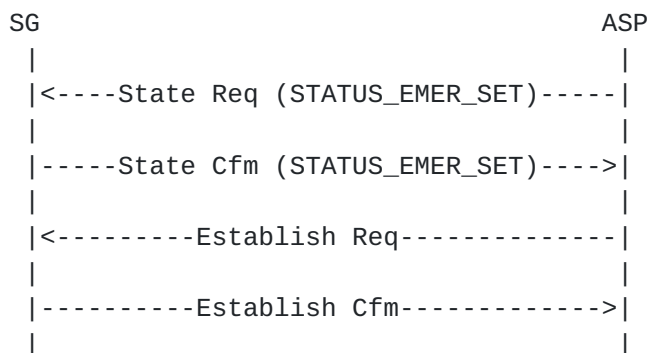
[5.3](#) SG to MGC, MTP Level 2 to MTP Level 3 Boundary Procedures

[5.3.1](#) SS7 Link Alignment

The MGC can request that a SS7 link be brought into alignment using the normal or emergency procedure. An example of the message flow to bring a SS7 link in-service using the normal alignment procedure is shown below.

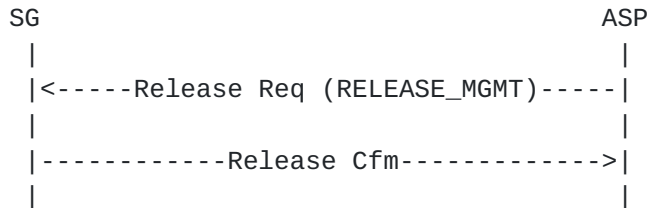


An example of the message flow to bring a SS7 link in-service using the emergency alignment procedure.

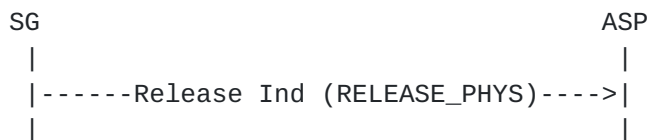


[5.3.2](#) SS7 Link Release

The MGC can request that a SS7 link be taken out-of-service. It uses the Release Request message as shown below.

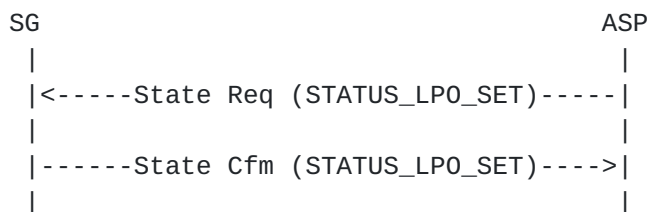


The SG can autonomously indicate that a SS7 link has gone out-of-service as shown below.

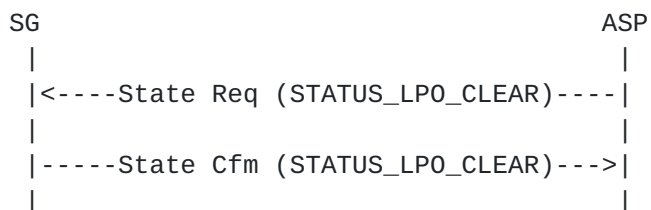


[5.3.3](#) Set and Clear Local Processor Outage

The MGC can set a Local Processor Outage condition. It uses the State Request message as shown below.

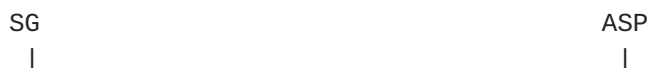


The MGC can clear a Local Processor Outage condition. It uses the State Request message as shown below.



[5.3.4](#) Notification of Processor Outage (local or remote)

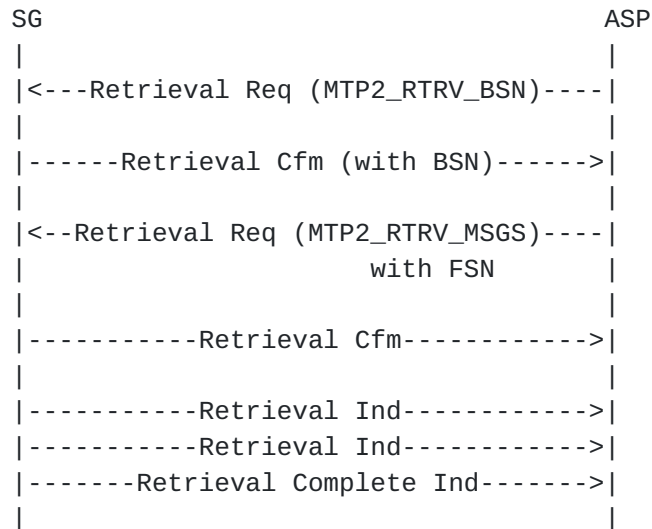
The SG can indicate a Local or Remote Processor Outage condition. It uses the State Indication message as shown below.



	-----State Ind (EVENT_ENTER_LP0)----->	
	-----State Ind (EVENT_EXIT_LP0)----->	
SG		ASP
	-----State Ind (EVENT_ENTER_RP0)----->	
	-----State Ind (EVENT_EXIT_RP0)----->	

5.3.5 SS7 Link Changeover

An example of the message flow for a changeover is shown below. In this example, there were three messages in the retransmission queue that needed to be retrieved.



Note: The number of Retrieval Indication is dependent on the number of messages in the retransmit queue that have been requested. Only one Retrieval Complete Indication should be sent.

6.0 Security

6.1 Introduction

M2UA is designed to carry signaling messages for telephony services. As such, M2UA 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, M2UA has the following security objectives:

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

M2UA runs on top of SCTP. SCTP [6] provides certain transport related security features, such as:

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

When M2UA 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" [[9](#)] should be consulted for guidance.

When the network in which M2UA 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 [\[10\]](#) 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 should be used instead. Regardless of which level performs the encryption, the IPSEC ISAKMP service should be used for key management.

[7.0](#) IANA Considerations

A request will be made to IANA to assign an M2UA value for the Payload Protocol Identifier in SCTP Payload Data chunk. The following SCTP Payload Protocol Identifier will be registered:

M2UA	tbd
------	-----

The SCTP Payload Protocol Identifier is included in each SCTP Data chunk, to indicate which protocol the SCTP is carrying. 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.

[8.0](#) Acknowledgements

The authors would like to thank Ian Rytina, Hanns Juergen Schwarzbauer and ZhangYi for their valuable comments and suggestions.

9.0 References

- [1] ITU-T Recommendation Q.700, 'Introduction To ITU-T Signalling System No. 7 (SS7)'
- [2] ITU-T Recommendation Q.701-Q.705, 'Signalling System No. 7 (SS7) - Message Transfer Part (MTP)'
- [3] ANSI T1.111 'Signalling System Number 7 - Message Transfer Part'
- [4] Bellcore GR-246-CORE 'Bell Communications Research Specification of Signaling System Number 7', Volume 1, December 1995
- [5] Framework Architecture for Signaling Transport, [draft-ietf-sigtran-framework-arch-03.txt](#), June 1999
- [6] Simple Control Transmission Protocol, [draft-ietf-sigtran-sctp-07.txt](#), March 2000
- [7] Media Gateway Control Protocol (MGCP), [draft-huitema-megaco-mgcp-v1-03.txt](#), August 1999
- [8] ITU-T Recommendation Q.2210, 'Message transfer part level 3 functions and messages using the services of ITU-T Recommendation Q.2140'
- [9] [RFC 2196](#), "Site Security Handbook", B. Fraser Ed., September 1997
- [10] [RFC 2401](#), "Security Architecture for the Internet Protocol", S. Kent, R. Atkinson, November 1998.

10.0 Author's Addresses

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

Tel: +1-703-484-3323
EMail: kmorneau@cisco.com

Malleswar Kalla
Telcordia Technologies
MCC 1J211R
445 South Street
Morristown, NJ 07960
USA

Tel: +1-973-829-5212
EMail: kalla@research.telcordia.com

Greg Sidebottom
Nortel Networks
3685 Richmond Rd,
Nepean, Ontario
Canada K2H5B7

Tel: +1-613-763-7305
EMail: gregside@nortelnetworks.com

Ram Dantu, Ph.D.
IPmobile
1651 North Glenville, Suite 216
Richardson, TX 75081
USA

Tel +1-972-234-6070 extension 211
EMail rdantu@ipmobile.com

Tom George
Alcatel USA
1000 Coit Road
Plano, TX 74075
USA

Tel: +1-972-519-3168
EMail: tom.george@usa.alcatel.com

This Internet Draft expires December 2000.