Network Working Group
INTERNET-DRAFT

Brian Bidulock
OpenSS7
Tom George
Alcatel
Ram Dantu
Netrake
Malleswar Kalla
Telcordia
Hanns Juergen Schwarzbauer
Siemens
Ken Morneault
Cisco Systems
Greg Sidebottom

Expires July 2003

January 7, 2003

SS7 MTP2-User Peer-to-Peer Adaptation Layer
M2PA
<draft-ietf-sigtran-m2pa-07.ps>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 or 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 supporting the transport of Signalling System Number 7 (SS7) Message Transfer Part (MTP) Level 3 signalling messages over Internet Protocol (IP) using the services of the Stream Control Transmission Protocol (SCTP). This protocol would be used between SS7 Signalling Points using the MTP Level 3 protocol. The SS7 Signalling Points may also use standard SS7 links using the SS7 MTP Level 2 to provide transport of MTP Level 3 signalling messages.

1. Introduction

1.1. Scope

There is a need for Switched Circuit Network (SCN) signalling protocol delivery over an IP network. This includes message transfer between the following:

- a Signalling Gateway (SG) and a Media Gateway Controller (MGC) [Q.700]
- a SG and an IP Signalling Point (IPSP)
- an IPSP and an IPSP

This could allow for convergence of some signalling and data networks. SCN signalling nodes would have access to databases and other devices in the IP network domain that do not use SS7 signalling links. Likewise, IP telephony applications would have access to SS7 services. There may also be operational cost and performance advantages when traditional signalling links are replaced by IP network “connections”.

The delivery mechanism described in this document allows for full MTP3 message handling and network management capabilities between any two SS7 nodes, communicating over an IP network. An SS7 node equipped with an IP network connection is called an IP Signalling Point (IPSP). The IPSPs function as traditional SS7 nodes using the IP network instead of SS7 links.

The delivery mechanism **SHOULD**

- Support seamless operation of MTP3 protocol peers over an IP network connection.
- Support the MTP Level 2 / MTP Level 3 interface boundary.
- Support management of SCTP transport associations and traffic instead of MTP2 Links.
- Support asynchronous reporting of status changes to management.

1.2. Change History

This section will be removed from the document when the document is finalized.

1.2.1. Changes from Version 0.6 to Version 0.7

- added this section
- reformatted document
- updated references and version number
- updated state transition diagrams
- changed timer names to align with Q.703 [Q.703]
- added proving state and procedure for timer T3
- fixed nits from the mailing list
- adjusted recommended timer values for alignment with Q.703 [Q.703]
- adjusted language on T7 timer to match WG comments
- created postscript diagrams
- spelling corrections

1.3. Terminology

MTP **–** The Message Transfer Part of the SS7 protocol [Q.701, Q.702, Q.703, Q.704..T1.111].

MTP2 **–** MTP Level 2, the MTP signalling link layer.

MTP3 **–** MTP Level 3, the MTP signalling network layer.

MTP2-User **–** A protocol that normally uses the services of MTP Level 2. The only MTP2 user is MTP3. The MTP2 user is equivalent to the M2PA user.

Signalling End Point (SEP) **–** A node in an SS7 network that originates or terminates signalling messages. One example is a central office switch.

IP Signalling Point (IPSP) **–** An SS7 Signalling Point with an IP network connection used for SS7 over IP.

Signalling Gateway (SG) **–** A signalling agent that receives/sends SCN native signalling at the edge of the IP network [RFC 2719]. In this context, an SG is an SS7 Signalling Point that has both an IP network connection used for SS7 over IP, and a traditional (non-IP) link to an SS7 network.

Signalling Transfer Point (STP) **–** A node in an SS7 network that routes signalling messages based on their destination point code in the SS7 network.

Association **–** An association refers to a SCTP association [RFC 2960]. The association provides the transport for MTP3 protocol data units and M2PA adaptation layer peer messages.

Network Byte Order **–** Most significant byte first, also known as “Big Endian”. See RFC 791 [RFC 791], Appendix B Data Transmission Order.

Stream **–** A stream refers to a SCTP stream [RFC 2960].

1.4. Abbreviations

BSNT	–	Backward Sequence Number to be Transmitted

FSNC	–	Forward Sequence Number of last message accepted by remote level 2
LI	–	Length Indicator
MSU	–	Message Signal Unit
SCCP	–	Signalling Connection Control Part
SCN	–	Switched Circuit Network
SCTP	–	Stream Control Transmission Protocol
SIF	–	Signalling Information Field
SIO	–	Service Information Octet
SLC	–	Signalling Link Code
SS7	–	Signalling System Number 7
SSN	–	Stream Sequence Number
STP	–	Signal Transfer Point

1.5. 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 RFC 2119 [RFC 2119].

1.6. Signalling Transport Architecture

The architecture that has been defined [RFC 2719] for Switched Circuit Network (SCN) signalling transport over IP uses multiple components, including an IP transport protocol, the Stream Control Transmission Protocol (SCTP), and an adaptation module to support the services expected by a particular SCN signalling protocol from its underlying protocol layer.

Within this framework architecture, this document defines an SCN adaptation module that is suitable for the transport of SS7 MTP3 messages.

Figure 1 shows the seamless interworking at the MTP3 layer. MTP3 is adapted to the SCTP layer using the MTP2 User Peer-to-peer Adaptation Layer (M2PA). All the primitives between MTP3 and MTP2 are supported by M2PA. The SCTP association acts as one SS7 link between the IPSPs. An IPSP **MAY** have the Signalling Connection Control Part (SCCP) and other SS7 layers above MTP3.

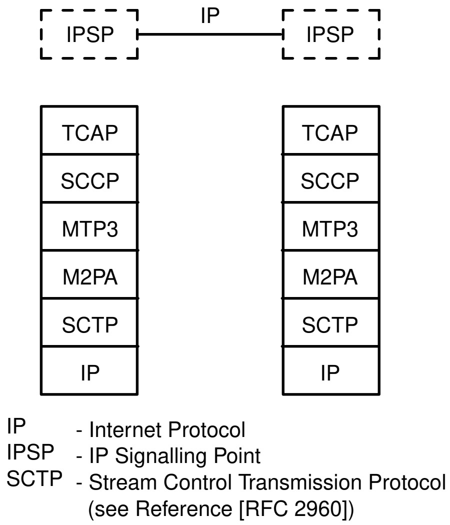

Figure 1. M2PA Symmetrical Peer-to-Peer Architecture

Figure 2 shows an example of M2PA used in a Signalling Gateway (SG). The SG is an IPSP equipped with both traditional SS7 and IP network connections. In effect, the Signalling Gateway acts as a Signal Transfer Point (STP). Any of the nodes in the diagram could have SCCP or other SS7 layers. STPs **MAY** or **MAY NOT** be present in the SS7 path between the SEP and the SG.

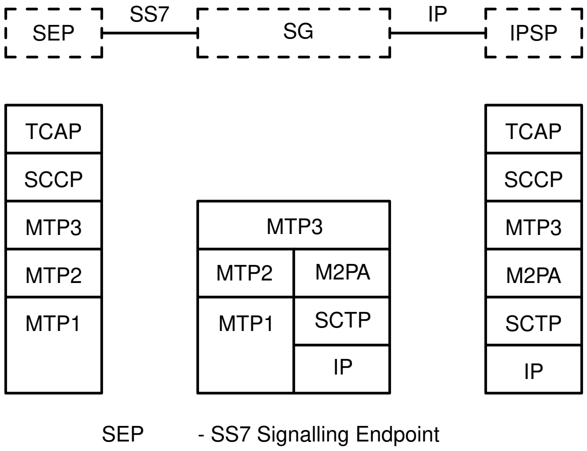

Figure 2. M2PA in IP Signalling Gateway

Figure 2 only an example. Other configurations are possible. In short, M2PA uses the SCTP association as an SS7 link. The M2PA/SCTP/IP stack can be used in place of an MTP2/MTP1 stack.

1.6.1. Point Code Representation

The MTP specification requires that each node with an MTP3 layer is identified by an SS7 point code. In particular, each IPSP **MUST** have its own SS7 point code.

1.7. Services Provided by M2PA

The SS7 MTP3/MTP2 (MTP2-User) interface is retained in the IPSP. The M2PA protocol layer is required to provide the equivalent set of services to its user as provided by MTP Level 2 to MTP Level 3.

These services are described in the following subsections.

1.7.1. Support for MTP Level 2 / MTP Level 3 interface boundary

This interface is the same as the MTP2/MTP3 interface described in Q.701 through Q.705 [Q.701, Q.702, Q.703, Q.704..T1.111], and Q.2140 [Q.2140], with the addition of support for larger sequence numbers in T1.111 [T1.111] and Q.2210 [Q.2210].

Because M2PA uses larger sequence numbers than MTP2, the MTP3 Changeover procedure **MUST** use the Extended Changeover Order and Extended Changeover Acknowledgment messages described in Q.2210 [Q.2210] and T1.111 [T1.111].

Also, the following MTP3/MTP2 primitives **MUST** use the larger sequence numbers:

- BSNT Confirmation
- Retrieval Request and FSNC

1.7.2. Support for peer-to-peer communication

In SS7, MTP Level 2 sends three types of messages, known as signal units: Message Signal Units (MSUs), Link Status Signal Units (LSSUs), and Fill-In Signal Units (FISUs).

MSUs originate at a higher level than MTP2, and are destined for a peer at another node. Likewise, M2PA passes these messages from MTP3 to SCTP as data for transport across a link. These are called User Data messages in M2PA.

LSSUs allow peer MTP2 layers to exchange status information. Analogous messages are needed for M2PA. The Link Status message serves this purpose.

FISUs are sent when no other signal units are waiting to be sent. This purpose is served by the heartbeat messages in SCTP. FISUs also carry acknowledgment of messages. This function is performed by the M2PA User Data and Link Status messages. Therefore, it is unnecessary for M2PA to provide a protocol data unit like the FISU. Furthermore, since an IP network is a shared resource, it would be undesirable to have a message type that is sent continuously as the FISUs are.

1.8. Functions Provided by M2PA

1.8.1. Support of MTP3/MTP2 Primitives

M2PA receives the primitives sent from MTP3 to its lower layer. M2PA processes these primitives or maps them to appropriate primitives at the M2PA/SCTP interface. Likewise, M2PA sends primitives to MTP3 like those used in the MTP3/MTP2 interface.

1.8.2. MTP2 Functionality

M2PA provides MTP2 functionality that is not provided by SCTP. This includes

- Data retrieval to support the MTP3 changeover procedure
- Reporting of link status changes to MTP3
- Processor outage procedure
- Link alignment procedure

SCTP provides reliable, sequenced delivery of messages.

1.8.3. Mapping of SS7 and IP Entities

The M2PA layer **MUST** maintain a map of each of its SS7 links to the corresponding SCTP association.

1.8.4. SCTP Stream Management

SCTP allows a user-specified number of streams to be opened during the initialization. It is the responsibility of the M2PA layer to ensure proper management of the streams allowed within each association.

M2PA uses two streams in each direction for each association. Stream 0 in each direction is designated for Link Status messages. Stream 1 is designated for User Data messages. Separating the Link Status and User Data messages onto separate streams allows M2PA to prioritize the messages in a manner similar to MTP2.

1.8.5. Retention of MTP3 in the SS7 Network

M2PA allows MTP3 to perform all of its Message Handling and Network Management functions with IPSPs as with other SS7 nodes.

1.9. Definition of the M2PA Boundaries

1.9.1. Definition of the M2PA / MTP Level 3 boundary

The upper layer primitives provided by M2PA are the same as those provided by MTP2 to MTP3. These primitives are described in Q.701 through Q.705 [Q.701, Q.702, Q.703, Q.704, Q.705], and T1.111 [T1.111]. and Q.2140 [Q.2140]. Following is a list of the primitives.

Primitives sent from MTP3 to M2PA:

Data Request	Used to send a Data Message for transmission.
Start Request	Used to activate a link.
Stop Request	Used to deactivate a link.
Retrieve BSNT Request	Request the BSNT for the changeover procedure.
Retrieval Request and FSNC	Request retrieval of unacknowledged and unsent messages. This request includes the FSNC received from the remote end.
Local Processor Outage Request	Informs M2PA of a local processor outage condition.
Local Processor Outage Recovered Request	Informs M2PA that a local processor outage condition has ceased.

Flush Buffers Request	Requests that all transmit and receive buffers be emptied.
Continue Request	Requests that processing resume after a processor outage.
Emergency Request	Requests that M2PA use the emergency alignment procedure.
Emergency Ceases Request	Requests that M2PA use the normal alignment procedure.

Primitives sent from M2PA to MTP3:

Data Indication	Used to deliver received Data Message to MTP3.
Congestion Indication	Indicates change in congestion status. The indication includes the congestion status, if the protocol is using the **OPTIONAL** congestion levels. The indication also includes the discard status.
In Service Indication	Indicates that the link is in service.
Out of Service Indication	Indicates that the link is out of service.
Retrieved Messages Indication	Indicates delivery of unacknowledged and unsent messages.
Retrieval Complete Indication	Indicates that delivery of unacknowledged and unsent messages is complete.
BSNT Confirm	Replies to the BSNT Request. The confirmation includes the BSNT.
BSNT Not Retrievable Confirm	Replies to the BSNT Request when the BSNT cannot be determined.
Remote Processor Outage Indication	Indicates processor outage at remote end.
Remote Processor Recovered Indication	Indicates recovery from processor outage at remote end.

1.9.2. Definition of the Lower Layer Boundary between M2PA and SCTP

The upper layer primitives provided by SCTP are described in RFC 2960 [RFC 2960] Section 10 “Interface with Upper Layer”.

1.10. Differences Between M2PA and M2UA

The MTP2 User Adaptation Layer (M2UA) [M2UA] also adapts the MTP3 layer to the SCTP/IP stack. It does so through a backhauling architecture [RFC 2719]. This section intends to clarify some of the differences between the M2PA and M2UA approaches.

A possible M2PA architecture is shown in *Figure 3*. Here the IPSPs MTP3 uses its underlying M2PA as a replacement for MTP2. Communication between the two layers MTP3/M2PA is defined by the same primitives as in SS7 MTP3/MTP2. M2PA performs functions similar to MTP2.

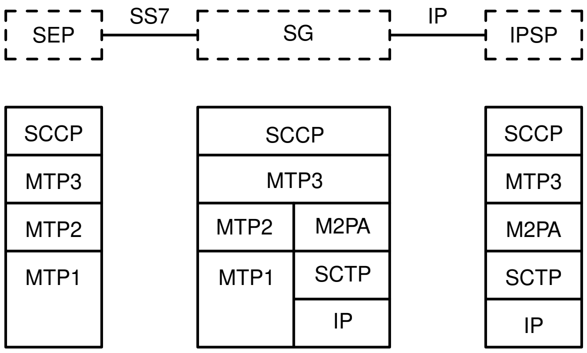

Figure 3. M2PA in IP Signalling Gateway

A comparable architecture for M2UA is shown in *Figure 4*. In M2UA, the MGCs MTP3 uses the SG's MTP2 as its lower SS7 layer. Likewise, the SG's MTP2 uses the MGCs MTP3 as its upper SS7 layer. In SS7, communication between the MTP3 and MTP2 layers is defined by primitives. In M2UA, the MTP3/MTP2 communication is defined as M2UA messages and sent over the IP connection.

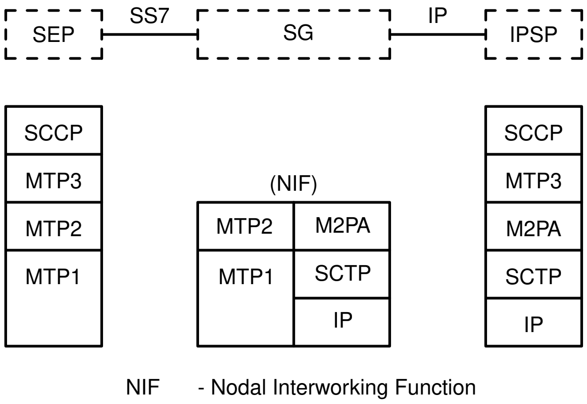

Figure 4. M2UA in IP Signalling Gateway

M2PA and M2UA are similar in that:

a.	Both	Transport MTP3 data messages.
b.	Both	Present an MTP2 upper interface to MTP3.

Differences between M2PA and M2UA include:

a.	M2PA:	IPSP processes MTP3/MTP2 primitives.
	M2UA:	MGC transports MTP3/MTP2 primitives between the SG's MTP2 and the MGCs MTP3 (via the NIF) for processing.
b.	M2PA:	SG-IPSP connection is an SS7 link.
	M2UA:	SG-MGC connection is not an SS7 link. It is an extension of MTP to a remote entity.
c.	M2PA:	SG is an SS7 node with a point code.
	M2UA:	SG is not an SS7 node and has no point code.
d.	M2PA:	SG can have upper SS7 layers, e.g., SCCP.
	M2UA:	SG does not have upper SS7 layers since it has no MTP3.
e.	M2PA:	relies on MTP3 for management procedures.
	M2UA:	uses M2UA management procedures.

Potential users of M2PA and M2UA **SHOULD** be aware of these differences when deciding how to use them for SS7 signalling transport over IP networks.

2. Protocol Elements

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

All fields in an M2PA message **MUST** be transmitted in the network byte order, i.e., most significant byte first, unless otherwise stated.

2.1. Common Message Header

The protocol messages for M2PA require a message header structure which contains a version, message class, message type, and message length. The header structure is shown in *Figure 5*.

```
 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    |     Spare     | Message Class | Message Type  |
+- - - - - - - -+- - - - - - - -+- - - - - - - -+- - - - - - - -+
|                        Message Length                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5. Common Message Header

2.1.1. Version

The version field contains the version of M2PA. The supported versions are:

Value (decimal)	Version
1	Release 1.0 of M2PA protocol

2.1.2. Spare

The Spare field **SHOULD** be set to all zeroes (0's) by the sender and ignored by the receiver. The Spare field **SHOULD NOT** be used for proprietary information.

2.1.3. Message Class

The following List contains the valid Message Classes:

Value (decimal)	Message Class
11	M2PA Messages

Other values are invalid for M2PA.

2.1.4. Message Type

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

Value (decimal)	Message Type
1	User Data
2	Link Status

Other values are invalid.

2.1.5. Message Length

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

2.2. M2PA Header

All protocol messages for M2PA require an M2PA-specific header. The header structure is shown in *Figure 6*.

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     unused    |                      BSN                      |
+- - - - - - - -+- - - - - - - - - - - - - - - - - - - - - - - -+
|     unused    |                      FSN                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6. M2PA-specific Message Header

2.2.1. Backward Sequence Number

This is the FSN of the message last received from the peer.

2.2.2. Forward Sequence Number

This is the M2PA sequence number of the User Data message being sent.

2.3. M2PA Messages

The following section defines the messages and parameter contents. An M2PA message consists of a Common Message Header and M2PA Header followed by the data appropriate to the message.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                               \
/                     Common Message Header                     /
\                                                               \
+- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
\                                                               \
/                  M2PA-specific Message Header                 /
\                                                               \
+- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
/                                                               /
\                                                               \
/                         Message Data                          /
\                                                               \
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

2.3.1. User Data

The User Data is the data sent from MTP3. The format for the User Data 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                                               /
\                                                               \
/                              Data                             /
\                                                               \
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The Data field contains the following fields of the MTP Message Signal Unit (MSU):

- Length Indicator (LI), including the two undefined bits between the SIO and LI fields.
- Service Information Octet (SIO)
- Signalling Information Field (SIF)

The MTP MSU described in Q.703 [Q.703], section 2.2 Signal Unit Format, and T1.111.3 [T1.111] section 2.2 Signal Unit Format.

M2PA does not add padding to the MTP3 message.

Note that the Data field **SHALL NOT** contain other components of the MTP MSU format:

- Flag
- Backward Sequence Number (BSN)
- Backward Indicator Bit (BIB)
- Forward Sequence Number (FSN)
- Forward Indicator Bit (FIB)
- Check bits (CK)

The Data field **SHALL** be transmitted in the byte order as defined by MTP3.

It is not necessary to put the message length in the LI octet as in MTP2. The LI octet is included because the two spare bits in the LI octet are used by MTP3 in at least one national version of SS7 to carry MTP3 information. For example, the Japanese TTC standard uses these spare bits as an MTP3 Message Priority field. See JT-Q704 [JT-Q704], section 14 "Common Characteristics of message signal unit formats", section 14.2 (A) Priority Indicator (PRI). For versions of MTP that do not use these two bits, the entire octet is spare.

Therefore in M2PA the format of the LI octet is:

```
 0
 0 1 2 3 4 5 6 7
+-+-+-+-+-+-+-+-+
|PRI|   spare   | (followed by SIO, SIF)
+-+-+-+-+-+-+-+-+
```

PRI – Priority used only in national MTP defined in JT-Q704 [JT-Q704]. Spare for other MTP versions.

Since the LI octet is not used for a message length, there is no need to support the expanded LI field in Q.703 [Q.703], Annex A. Therefore the LI field in M2PA is always one octet.

Note: In the SS7 Recommendations, the format of the messages and fields within the messages are based on bit transmission order. In these recommendations the Least Significant Bit (LSB) of each field is positioned to the right. The received SS7 fields are populated octet by octet as received into the 4-octet word as shown below.

As an example, in the ANSI MTP protocol, the Data field format is shown below:

```
|MSB-------------------------------------------------------LSB|
 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
 .)b
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|PRI|   spare   |      SIO      |   SIF octet   |      ...      |
+- -+- - - - - -+- - - - - - - -+- - - - - - - -+- - - - - - - -+
\                               .                               \
/                               .                               /
\                               .                               \
+- - - - - - - -+- - - - - - - -+- - - - - - - -+- - - - - - - -+
|      ...      |      ...      |      ...      |   SIF octet   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Within each octet the Least Significant Bit (LSB) per the SS7 Recommendations is to the right (e.g., bit 15 of SIO is the LSB).

2.3.2. Link Status

The MTP2 Link Status message can be sent between M2PA peers to indicate link status. This message performs a function similar to the the Link Status Signal Unit in MTP2. The format for the Link Status 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             State                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

Value (decimal)	Description
1	Alignment
2	Proving Normal
3	Proving Emergency
4	Ready
5	Processor Outage
6	Processor Outage Ended
7	Busy
8	Busy Ended
9	Out of Service

2.3.2.1. Link Status Proving

The Link Status Proving message **MAY OPTIONALLY** carry additional bytes. If the **OPTIONAL** bytes are used, the format for the 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             State                             |
+- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -+
\                                                               \
/                             filler                            /
\                                                               \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

It is **RECOMMENDED** that the length of the Link Status Proving message be similar to the size of the User Data messages that will be carried on the link.

It is **RECOMMENDED** that the filler field contain a number pattern which varies among the Link Status Proving messages, and that will allow the SCTP checksum to be used to verify the accuracy of transmission.

3. M2PA Link State Control

The M2PA link moves from one state to another in response to various events. The events that **MAY** result in a change of state include:

- MTP3 primitive requests
- SCTP notifications
- Receipt of Status messages from the peer M2PA
- Expiration of certain timers

Figure 7 illustrates state changes together with the causing events. Note that some of the error conditions are not shown in the state diagram.

Following is a list of the M2PA Link States and a description of each.

POWER OFF – State of the link during power-up initialization.

OUT OF SERVICE – Out Of Service. Power-up initialization is complete.

INITIAL ALIGNMENT – Alignment In Progress. M2PA is attempting to exchange Alignment messages with its peer.

PROVING – M2PA is sending Link Status Proving messages to its peer.

ALIGNED READY – Proving is complete. M2PA is waiting until peer completes proving.

ALIGNED NOT READY – Proving is complete, but local or remote processor is out.

IN SERVICE – In Service. Link is ready for traffic.

PROCESSOR OUTAGE – In Service, but the local or remote processor is out.

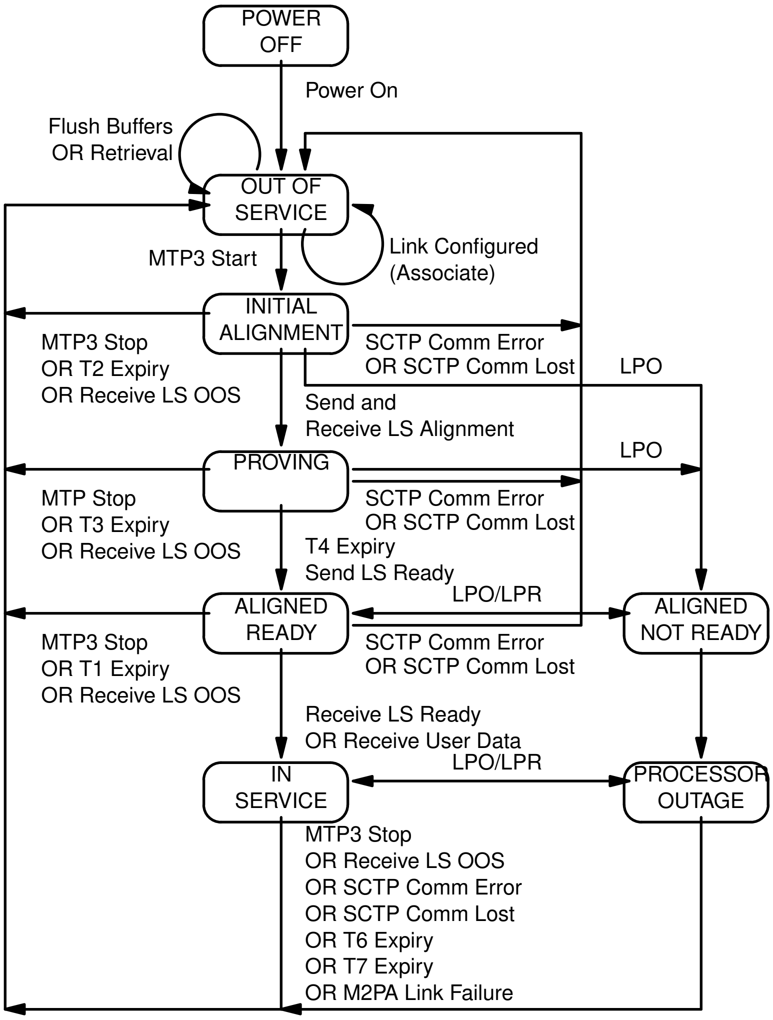

Figure 7. M2PA Link State Transition Diagram

Figure 8 illustrates state changes in the M2PA management of the SCTP association together with the causing events. Note that some of the error conditions are not shown in the state diagram.

Following is a list of the M2PA Association States and a description of each.

IDLE – State of the association during power-up initialization.

ASSOCIATE – M2PA is attempting to establish an SCTP association.

ESTABLISHED – SCTP association is established.

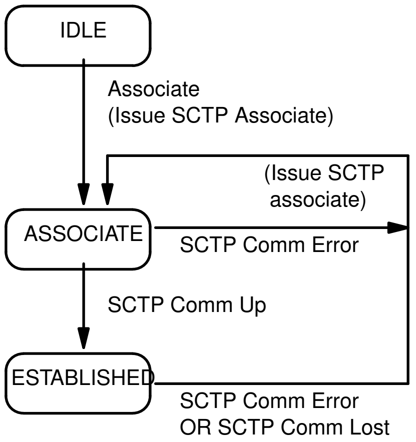

Figure 8. M2PA Association State Transition Diagram

4. Procedures

4.1. Procedures to Support MTP2 Features

4.1.1. Signal Unit Format, Delimitation, Acceptance

Messages for transmission across the network **MUST** follow the format described in section 2.

SCTP provides reliable, in-sequence delivery. Therefore the related functionality of MTP2 is not needed. SCTP does not provide functions related to Link State Control in MTP2. These functions **MUST** be provided by M2PA.

4.1.2. MTP and SCTP Entities

This section describes how M2PA relates MTP and SCTP entities.

Each MTP link corresponds to an SCTP association. To prevent duplicate associations from being established, it is **RECOMMENDED** that each endpoint know the IP address (or IP addresses, if multi-homing is used) and port number of both endpoints. SCTP prevents two associations with the same IP addresses and port numbers from being established.

It is necessary for at least one of the endpoints to be listening on the port on which the other endpoint is trying to establish the association. Therefore, at least one of the port numbers **SHOULD** be the M2PA registered port.

If only one association is to be established between these two IP addresses, then the association **SHOULD** be established using the M2PA registered port at each endpoint.

If it is desirable to create multiple associations (for multiple links) between the two IP addresses, different port numbers can be used for each association. Nevertheless, the M2PA registered port number **SHOULD** be used at one end of each association.

Each combination of IP address/port for the two endpoints (i.e., each association) **MUST** be mapped to the same Signalling Link Code (SLC) at each endpoint, so that each endpoint knows which link is being created at the time the SCTP association is established. However, M2PA does not do any processing based on the SLC.

Following are examples of the relationships between associations and links. Note that a link is an SCTP association identified by two endpoints. Each endpoint is identified by an IP address and port number. Each association is mapped to an SLC.

Figure 9 shows a case with two IPSPs, each with two IP addresses. Two associations are the links that connect the two IPSPs. Since these links are in the same link set, they **MUST** have different SLCs.

Table 1 shows the relationships in tabular form. *Table 1* is only conceptual. The actual method for mapping the SCTP associations to the SLCs is implementation dependent.

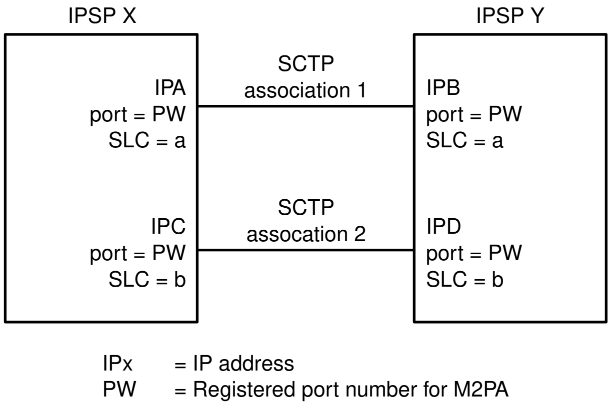

Figure 9. Two IPSPs with Two IP Addresses Each

Table 1. Two IPSPs with Two IP Addresses Each

Association	IPSP X		IPSP Y		SLC
	IP address	Port	IP address	Port	
1	IPA	PW	IPB	PW	a
2	IPC	PW	IPD	PW	b

Figure 10 and *Table 2* show an example with three IPSPs. Note that in this example, the two links are in different link sets. Therefore, it is possible that the values a and b **MAY** be equal.

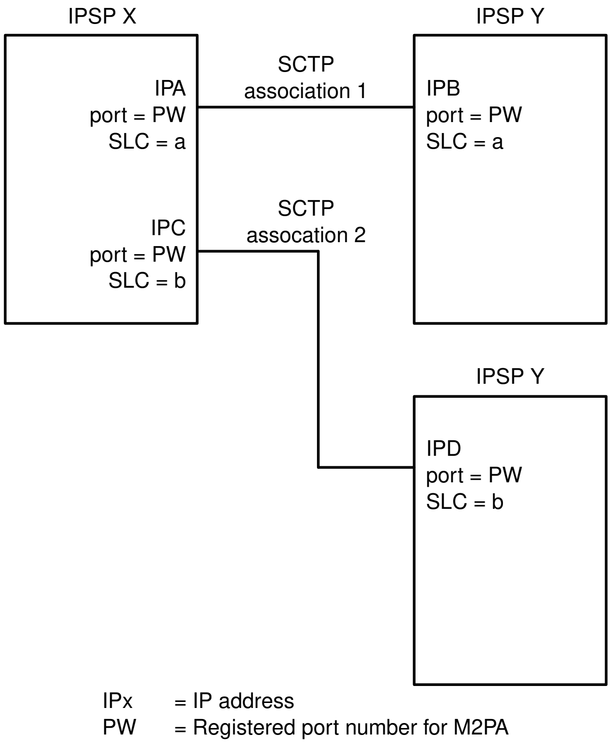

Figure 10. One IPSP Connected to Two IPSPs

Table 2. One IPSP Connected to Two IPSPs

Association	**IPSP X**		**IPSP Y**		**SLC**
	IP address	**Port**	**IP address**	**Port**	
1	IPA	PW	IPB	PW	a
2	IPC	PW	IPD	PW	b

Figure 11 and *Table 3* show two associations between the same IP addresses. This is accomplished by using different port numbers for each association at one endpoint.

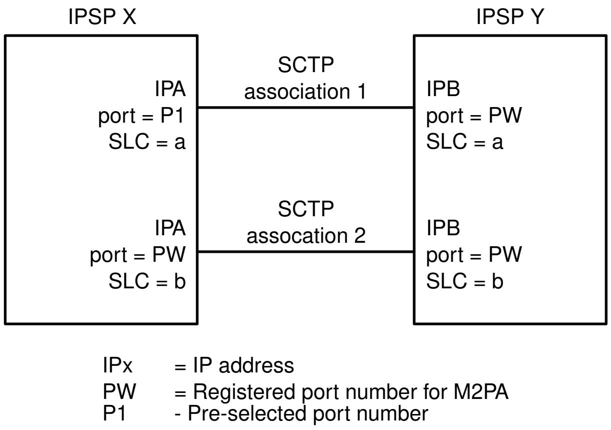

Figure 11. Multiple Associations Between Two IP Addresses

Table 3. Multiple Associations Between Two IP Addresses

Association	**IPSP X**		**IPSP Y**		**SLC**
	IP address	**Port**	**IP address**	**Port**	
1	IPA	P1	IPB	PW	a
2	IPA	PW	IPB	PW	b

The association **SHALL** contain two streams in each direction. Stream 0 is designated for Link Status messages. Stream 1 is designated for User Data messages.

4.1.3. Link Alignment

The purposes of the alignment procedure are:

(1) To provide a handshaking procedure so that both endpoints are prepared to send SS7 traffic, and to prevent traffic from being sent before the other end is ready.

(2) To verify that the SCTP association is suitable for use as an SS7 link.

Link alignment takes place after the association is established. If SCTP fails to establish the association, and M2PA has received a Start Request from its MTP3, then M2PA **SHALL** report to MTP3 that the link is out of service.

After the association is established, M2PA **SHALL** send a Link Status Out of Service message to its peer.

Once the association is established and M2PA has received a Start Request from MTP3, M2PA sends the Link Status Alignment message to its peer. If M2PA has not already received the Link Status Alignment message from its peer, then M2PA starts timer T2.

(Note that if the remote M2PA has not received a Start Request from its MTP3, it will not send the Link Status Alignment message to the local M2PA. Eventually timer T2 in the local M2PA will expire. If the remote M2PA receives a Start Request from its MTP3 and sends Link Status Alignment before the local M2PA timer T2 expires, the alignment procedure can continue.)

M2PA stops timer T2 when it has received the Link Status Alignment message from its peer.

If timer T2 expires, then M2PA reports to MTP3 that the link is out of service. M2PA sends Link Status Out of Service to its peer. M2PA **SHOULD** leave the association established. M2PA waits for MTP3 to initiate the alignment procedure again.

Note: Between the time M2PA sends Link Status Alignment to its peer and receives Link Status Alignment from its peer, M2PA **MAY** receive Link Status Out of Service from its peer. This message is ignored. After receiving Link Status Alignment from the peer, receipt of a Link Status Out of Service message causes M2PA to send Out of Service to MTP3 and return to the Out of Service state.

When M2PA has both sent and received the Link Status Alignment message, it has completed alignment. M2PA starts the aligned timer T3 and moves to the proving state.

M2PA stops timer T3 when it receives a Proving Normal or Proving Emergency message and starts proving period timer T4.

If timer T3 expires, then M2PA reports to MTP3 that the link is out of service. M2PA sends Link Status Out of Service to its peer. M2PA **SHOULD** leave the association established. M2PA waits for MTP3 to initiate the alignment procedure again.

M2PA starts the proving period timer T4. During the proving period, M2PA sends Link Status Proving messages to its peer at an interval defined by the protocol parameter Proving_Rate. M2PA sends either the Proving Normal or Proving Emergency message, according to the Emergency and Emergency Ceases commands from MTP3. M2PA uses the value of T4 corresponding to the Normal or Emergency state. However, if M2PA receives a Link Status Proving Emergency message from its peer, then M2PA **SHALL** initiate the Emergency proving period value for T4, but it **SHALL** continue to send the Proving message (Normal or Emergency) determined by its own upper layer MTP3.

When the proving period timer T4 expires, M2PA **SHALL** start the timer T1 and send Link Status Ready messages to its peer at interval Status_Interval. These messages are used to verify that both ends have completed proving.

M2PA **SHALL** stop timer T1 when it receives a Link Status Ready or User Data message from its peer. If timer T1 expires, then M2PA reports to MTP3 that the link is out of service. M2PA sends Link Status Out of Service to its peer. M2PA **SHOULD** leave the association established. M2PA waits for MTP3 to initiate the alignment procedure again.

Note that if M2PA has already received a Link Status Ready message from its peer when its timer T4 expires, there is no need to start timer T1. M2PA can just send Link Status Ready to the peer and continue along.

When all of the following are true:

(a) M2PA has received a Start Request from MTP3.

(b) M2PA proving period T4 has expired.

(c) M2PA has sent a Link Status Ready to its peer.

(d) M2PA has received a Link Status Ready OR User Data message from its peer.

(e) M2PA has not received Link Status Out of Service from its peer since it received Link Status Alignment.

then M2PA **SHALL** send Link In Service to its MTP3.

If there is a local processor outage condition during the alignment procedure, M2PA sends Link Status Processor Outage to its peer. When the local processor outage condition ends, then M2PA **SHALL** send Link Status Processor Outage Ended to its peer. M2PA **SHALL** attempt to complete the alignment procedure during the local processor outage condition.

If M2PA receives a Link Status Processor Outage during alignment, and M2PA had received a Start Request from its MTP3, M2PA **SHALL** report Remote Processor Outage to MTP3. M2PA **SHALL** attempt to complete the alignment procedure during the remote processor outage condition.

If M2PA receives a Stop command from its MTP3 during alignment, M2PA **SHALL** send Link Status Out of Service to its peer and terminate the alignment procedure.

Anomalous messages received during alignment **SHOULD** be discarded. Examples include:

(a) User Data received before proving begins.

(b) Link Status Alignment received before or during proving.

Recommended values:

Table 4. Recommended Timer Values

Timer	(seconds)	
	Range	Default
T1 (Ready)	40 - 50	45
T2 (Not Aligned)	5 - 150	60
T3 (Aligned)	1.0 - 1.5	1.0
T4 (Normal)	7.5 - 9.5	8
T4 (Emerg)	0.400 - 0.600	0.500
Status_Interval	implementation dependent	
Proving_Rate	implementation dependent	

4.1.4. Processor Outage

A processor outage occurs when M2PA cannot transfer messages because of a condition at a higher layer than M2PA.

When M2PA detects a local processor outage, it sends a Link Status message to its peer with status Processor Outage. M2PA **SHALL** also cease sending User Data messages to SCTP for transmission. M2PA **SHALL** stop receiving incoming User Data messages from SCTP.

M2PA **SHOULD** periodically send a Link Status Processor Outage message as long as there is a local processor outage and the link is in service. If the link is out of service, M2PA **SHOULD** locally mark that it is in local processor outage.

The peer M2PA, upon receiving the Link Status Processor Outage message, **SHALL** report Remote Processor Outage to its MTP3. The peer M2PA ceases sending User Data messages. M2PA stops the Remote Congestion timer T6 (see section 4.1.5 Level 2 Flow Control) if it is running.

MTP3 **MAY** send a Flush Buffers or Continue command to M2PA as part of its processor outage procedure (See section 4.2.4 Flush Buffers, Continue). Alternatively, MTP3 **MAY** perform data retrieval as part of a changeover procedure.

When the processor outage ceases, MTP3 sends a Local Processor Recovered indication to M2PA. The local M2PA notifies its peer by sending a Link Status message with status Processor Outage Ended. The peer uses the Remote Processor Recovered Indication to notify its MTP3 that the remote processor outage condition has ceased.

4.1.5. Level 2 Flow Control

The determination of receive congestion in M2PA is implementation dependent.

If M2PA determines that it is in receive congestion for an association, M2PA **SHALL** send a Link Status Busy message to its peer on that association. M2PA **SHALL** continue to acknowledge incoming messages.

M2PA **SHOULD** periodically send a Link Status Busy message as long as it is in receive congestion.

M2PA **SHALL** continue transmitting messages while it is in receive congestion.

When the peer M2PA receives the Link Status Busy message, it **SHALL** start the Remote Congestion timer T6. If timer T6 expires, M2PA **SHALL** take the link out of service. M2PA sends a Link Status Out of Service message to its peer, and goes to the Retrieval state.

The peer M2PA **SHOULD** continue transmitting messages to SCTP while its T6 timer is running, i.e., while the other end is Busy.

The peer M2PA **SHALL** not fail the link due to expiration of timer T7 excessive delay of acknowledgment (see section 4.2.1 Sending and receiving messages) while its T6 timer is running, i.e., while the other end is Busy.

If M2PA is no longer in receive congestion for the association, M2PA **SHALL** send a Link Status Busy Ended message to its peer on that association.

When the peer M2PA receives the Link Status Busy Ended message, it **SHALL** stop timer T6.

Recommended values:

Table 5. Recommended Timer Values

Timer	(seconds)	
	Range	Default
T6 (Busy)	3.0 - 6.0	4.5

4.1.6. Error Monitoring

If M2PA loses the SCTP association for a link, M2PA **SHALL** report to MTP3 that the link is out of service.

4.1.7. Transmission and Reception Priorities

In MTP, Link Status messages have priority over User Data messages (Q.703 [Q.703], section 11.2). To achieve this in M2PA, M2PA **SHALL** send Link Status and User Data messages on separate streams in its SCTP association. All messages are sent using the ordered delivery option.

M2PA **SHOULD** give higher priority to Link Status messages than to User Data messages when sending messages to SCTP.

M2PA **SHOULD** give higher priority to reading the Link Status stream than to reading the User Data stream.

M2PA **SHOULD** give higher priority to receiving notifications from SCTP than to reading either the Link Status stream or the User Data stream.

4.1.8. M2PA Version Control

A node upgraded to a newer version of M2PA **SHOULD** support the older versions used on other nodes with which it is communicating. If that is the case, then alignment can proceed normally.

In particular, it is **RECOMMENDED** that for future modifications to this protocol:

- Any newer version **SHOULD** be able to process the messages from a lower version.
- A newer version of M2PA **SHOULD** refrain from sending messages to an older version of M2PA messages that the older version cannot process.
- If an older version of M2PA receives a message that it cannot process, it **SHOULD** discard the message.
- In cases where different processing is done in two versions for the same format of a message, then the newer version **SHOULD** contain procedures to recognize this and handle it appropriately.

In case a newer version of M2PA is incompatible with an older version, the newer version **SHOULD** recognize this and prevent the alignment of the link. If a Link Status Alignment message with an unsupported version is received by the newer version, the receiving end's M2PA **SHALL** not complete the alignment procedure.

4.2. Procedures to Support the MTP3/MTP2 Interface

4.2.1. Sending and receiving messages

When MTP3 sends a message for transmission to M2PA, M2PA passes the corresponding M2PA message to SCTP using the SEND primitive.

M2PA Link Status messages are passed to SCTP using the SEND primitive.

Link Status and User Data messages **SHALL** be sent via SCTP on separate streams.

When M2PA receives a User Data message from SCTP, M2PA passes the message to MTP3.

If M2PA receives a message from SCTP with an invalid Message Class or unsupported Message Type in the Common Message Header, M2PA **SHALL** discard the message.

The first User Data message sent after the link is placed in service is given a Forward Sequence Number (FSN) of 1.

The Forward Sequence Number of the header is incremented by 1 for each User Data message sent. When the FSN reaches the maximum value, the next FSN is 0.

For message types other than User Data, the Forward Sequence Number is set to the FSN of the last User Data message sent.

The Backward Sequence Number is set to the FSN of the last User Data message M2PA received from its peer. This serves as an M2PA-level acknowledgment of the message. After the link is placed in service and before a User Data message has been received, the BSN is set to 0.

When M2PA receives a User Data message with Backward Sequence Number equal to its queue.

If M2PA receives a User Data message with an FSN that is out of order, M2PA **SHALL** fail the link.

M2PA **SHOULD** follow the criterion stated in Q.703 [Q.703], section 5.3.1 for incorrect BSNs: If any two BSNs in three consecutively received User Data messages are not the same as the previous one or any of the FSNs of the User Data messages in the M2PA retransmit buffer at the time they are received, then MTP3 **SHOULD** be informed that the link is faulty.

M2PA **SHOULD** ignore the FSN and BSN contained in a Link Status message.

Note: In all calculations involving FSN and BSN, the programmer **SHOULD** be aware that the value wraps around to 0 after reaching its maximum value.

If there is no other User Data message to be sent when there is a message to acknowledge, M2PA **MAY** send a User Data message with no data payload. The FSN for this empty User Data message is not incremented. It **MUST** contain the same FSN as the most recently sent User Data message containing Data.

If M2PA receives an empty User Data message, it **SHALL** not send an acknowledgment of that message.

Note that there is no reason to place empty User Data messages in the MT2PA transmit buffer, since the empty messages are not retransmitted and timer T7 (below) does not apply to them.

Note that since SCTP provides reliable delivery and ordered delivery within the stream, M2PA does not perform retransmissions.

Timer T7 provides an indication of excessive delay of acknowledgment. If the following conditions are true:

(a) There is at least one message in the M2PA retransmit buffer.

(b) The remote M2PA is not in a Busy condition (i.e. local timer T6 is not running).

(c) There is a message in the M2PA retransmit buffer that has not received an acknowledgment in the span of T7 since its last transmission.

Then M2PA **SHOULD** fail the link.

Recommended values:

Table 6. Recommended Timer Values

Timer	(seconds)			
	Range			Default
T7 (Ack)	0.5	-	2.0	1.0

4.2.2. Link activation and restoration

When MTP3 requests that M2PA activate or restore a link by a Start Request, M2PA **SHALL** follow the alignment procedure in section 4.1.3.

4.2.3. Link deactivation

When MTP3 requests that M2PA deactivate a link by a Stop command, M2PA **SHALL** send a Link Status Out of Service message to its peer.

The peer M2PA, upon receiving Link Status Out of Service, **SHALL** notify its upper layer MTP3 that the link is out of service.

4.2.4. Flush Buffers, Continue

The Flush Buffers and Continue commands allow M2PA to resume normal operations (i.e., transmission of messages to SCTP and receiving messages from SCTP) after a processor outage (local and/or remote) ceases.

If M2PA receives a Flush Buffers command from MTP3, M2PA:

(a) **SHALL** not transmit any messages to SCTP that are currently waiting to be transmitted to SCTP. These messages **SHALL** be discarded.

(b) **SHALL** discard all messages currently waiting to be passed to MTP3.

If M2PA receives either a Flush Buffers or Continue command from MTP3, and the processor outage condition ceases, M2PA **SHALL** resume receiving and transmitting messages.

4.2.5. MTP3 Signalling Link Congestion

M2PA **SHALL** detect transmit congestion in its buffers according to the requirements for signalling link transmit congestion in Q.704 [Q.704], section 3.8.

M2PA **SHALL** use the Congestion Indication primitive to notify its upper layer MTP3 of changes in the signalling link congestion status and the signalling link discard status. For national networks with multiple congestion threshold levels, M2PA **SHALL** notify MTP3 of the congestion and discard status levels.

4.2.6. Changeover

The objective of the changeover is to ensure that signalling traffic carried by the unavailable signalling link is diverted to the alternative signalling link(s) as quickly as possible while avoiding message loss, duplication, or mis-sequencing. For this purpose, the changeover procedure includes data retrieval, which is performed before opening the alternative signalling links to the diverted traffic. Data retrieval consists of these steps:

(1) buffer updating, i.e., identifying all those User Data messages in the retransmission buffer of the unavailable signalling link which have not been received by the far end M2PA, as well as not transmitted messages, and

(2) transferring those messages to the transmission buffers of the alternate links.

Note that only User Data messages are retrieved and transmitted over the alternate links. Link Status messages **SHALL** not be retrieved and transmitted over the alternate links.

M2PA Sequence Numbers are 24 bits long. MTP2's Forward and Backward Sequence Numbers are only seven bits long. Hence it is necessary for MTP3 to accommodate the larger sequence numbers. This is done through the use of the Extended Changeover Order (XCO) and Extended Changeover Acknowledgment (XCA) messages instead of the Changeover Order (COO) and Changeover Acknowledgment (COA) messages. The XCO and XCA messages are specified in Q.2210 [Q.2210], section 9.8.1 and Reference T1.111.4 [T1.111], section 15.4. Only the XCO and XCA messages from Q.2210 [Q.2210] or T1.111 [T1.111] are required. The BSN is placed in the XCO/XCA message as explained in Q.2210 [Q.2210] and T1.111 [T1.111].

Also, the following MTP3/MTP2 primitives **MUST** use the larger sequence numbers:

- BSNT Confirmation
- Retrieval Request and FSNC

For data retrieval, MTP3 requests the Backward Sequence Number to be Transmitted (BSNT) from M2PA through the Retrieve BSNT request. M2PA determines the Forward Sequence Number of the last User Data message received from the peer. This value is the BSNT. M2PA sends the BSNT value to MTP3 in the BSNT confirmation. In the same way, the remote end also detects its BSNT. The MTP3 layers exchange BSNT values through the XCO and XCA messages. The BSNT received from the other end is called the FSNC. When MTP3 receives the FSNC from the other end, MTP3 retrieves all the unsent and unacknowledged messages starting with sequence number (FSNC + 1). This is accomplished through a Retrieval Request and FSNC request. After all the messages are sent from M2PA to MTP3, M2PA sends a Retrieval Complete indication to MTP3.

If there are any messages on the M2PA or SCTP receive queues that have not been acknowledged by M2PA, M2PA **SHOULD** discard these messages. The peer will retransmit them on an alternate link. Any messages acknowledged by M2PA **MUST NOT** be discarded. These messages **MUST** be delivered to MTP3.

If M2PA receives a Retrieve BSNT request from MTP3, M2PA **SHALL** respond with the BSNT confirmation. The BSNT value is the Forward Sequence Number of the last User Data message received from the peer.

If M2PA receives a Retrieval Request and FSNC request from MTP3, M2PA **SHALL** retrieve from its buffers in order and deliver to MTP3:

(a) any transmitted User Data messages beginning with the first unacknowledged message with FSN greater than FSNC.

(b) any not transmitted User Data messages.

Then M2PA **SHALL** send the Retrieval Complete indication to MTP3.

For emergency changeover, MTP3 retrieves only the unsent messages for transmission on the alternate link(s). If M2PA receives a Retrieval Request and FSNC request with no FSNC value, or with an invalid FSNC, then M2PA **SHALL** retrieve from its buffers in order and deliver to MTP3:

(a) any not transmitted User Data messages.

Then M2PA **SHALL** send the Retrieval Complete indication to MTP3.

Note: For the Japanese version of MTP defined in JT-Q704 [JT-Q704], MTP3 retrieves both unsent and unacknowledged messages for transmission on the alternate link(s). In this version of MTP, if M2PA receives a Retrieval Request and FSNC request with no FSNC value, or with an invalid FSNC, then M2PA **SHALL** retrieve from its buffers in order and deliver to MTP3:

(a) any transmitted but unacknowledged User Data messages.

(b) any not transmitted User Data messages.

Then M2PA **SHALL** send the Retrieval Complete indication to MTP3.

4.2.6.1. Multiple User Data Streams and Changeover

The changeover procedure makes it problematic for M2PA to have multiple User Data streams in one direction for a link. Buffer updating would have to be done for each User Data stream separately to avoid duplication or loss of messages. But MTP3 provides for only one XCO/XCA message for sending the last-received sequence number.

Even with sequence numbering of User Data messages at the M2PA layer, it is necessary to perform buffer updating on each stream. Since the M2PA messages would be delivered over multiple streams, there could be a gap in the M2PA sequence numbers at the receiving end when the changeover procedure begins. If only the M2PA sequence number is used in the XCO/XCA message, there would be a possibility of losing the messages in the gap, or duplicating messages after the gap.

M2PA links with multiple User Data streams would be possible if a multiple-BSNT XCO/XCA message is defined in MTP3, or MTP3 allows multiple XCO/XCA messages (one for each User Data stream) to be sent during a changeover. This is beyond the scope of this document.

4.3. SCTP Considerations

Some M2PA procedures **MAY** be affected by the use of SCTP as a transport layer. These considerations are discussed in this section.

4.3.1. SCTP Slow Start

SCTP contains a slow start algorithm to control the amount of data being injected into the network. The algorithm allows SCTP to probe the network to determine the available capacity. The algorithm is invoked when transmission begins on an association, after a sufficiently long idle period, or after repairing loss detected by the SCTP retransmission timer.

It is possible that transmission of M2PA messages **MAY** be delayed by SCTP slow start under certain conditions, including the following:

(a) Link Alignment. Link alignment takes place after an association is established. SCTP invokes the slow start algorithm since transmission is beginning on the association.

(b) Changeover. Messages are retrieved from one link (association) and transferred to another for transmission. If the second link had previously been idle, or is in the process of link alignment, SCTP **MAY** invoke the slow start algorithm.

(c) Path failure (multi-homing). If SCTP switches from a failed path to a new path, and the new path had previously been idle, SCTP **MAY** invoke the slow start algorithm.

(d) Reduced traffic volume. Any time that M2PA sends a low volume of traffic on a link and then the volume increases, SCTP **MAY** invoke the slow start algorithm.

Programmers **SHOULD** be aware of this condition and how it **MAY** affect M2PA performance. In some cases, it **MAY** be possible to avoid the negative effects of slow start. For example, the Link Status Proving messages sent during the proving period **MAY** be used to complete slow start before the link is placed in service.

5. Examples of M2PA Procedures

In general, messages passed between MTP3 and M2PA are the same as those passed between MTP3 and MTP2. M2PA interprets messages from MTP3 and sends the appropriate message to SCTP. Likewise, messages from SCTP are used to generate a meaningful message to MTP3.

Note that throughout this section, the primitives between MTP3 and M2PA are named using the MTP terminology [Q.700, Q.701, Q.702, Q.703, Q.704, Q.705]. Communications between M2PA and SCTP are named using SCTP terminology.

5.1. Link Initialization (Alignment)

An example of the message flow to bring an SS7 link in service is shown below. Alignment is done by both ends of the link. To simplify the diagram, alignment is shown on one end only. It is assumed in this example that SCTP has been initialized.

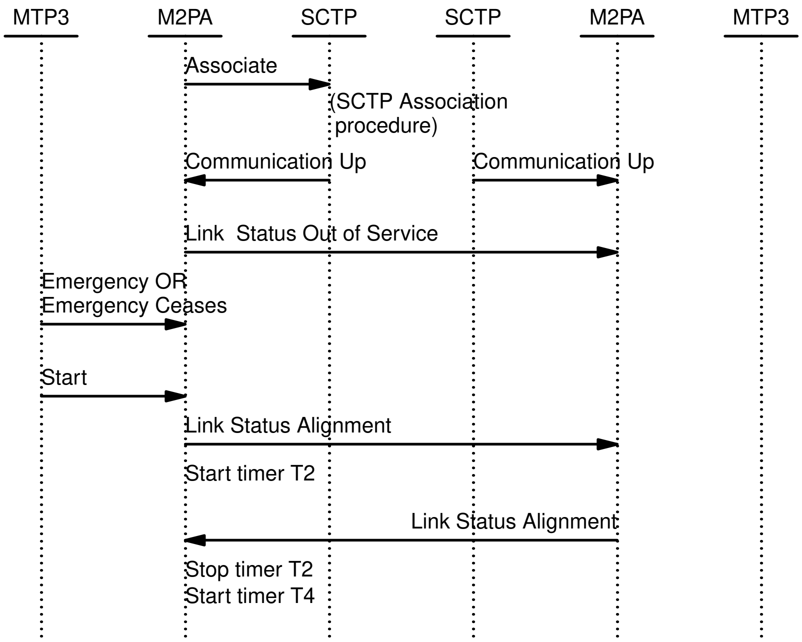

Figure 12. Example: Link Initialization – Alignment

Proving period begins. (Messages from remote end not shown.)

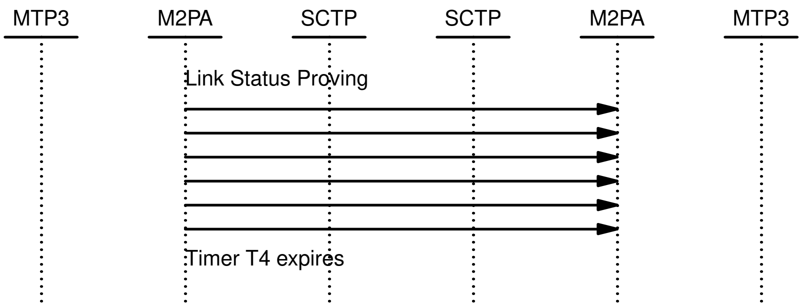

Figure 13. Example: Link Initialization – Proving

Send Link Status Ready until the remote end completes its proving period.

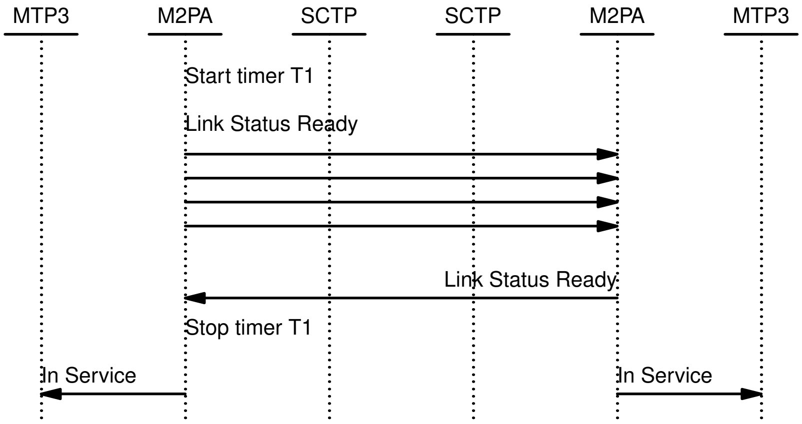

Figure 14. Example: Link Initialization – In Service

At this point, MTP3 **MAY** begin sending data messages.

5.2. Message Transmission and Reception

Messages are transmitted using the Data Request primitive from MTP3 to M2PA. The diagram shows the case where the Link is In Service. The message is passed from MTP3 of the source to MTP3 of the destination.

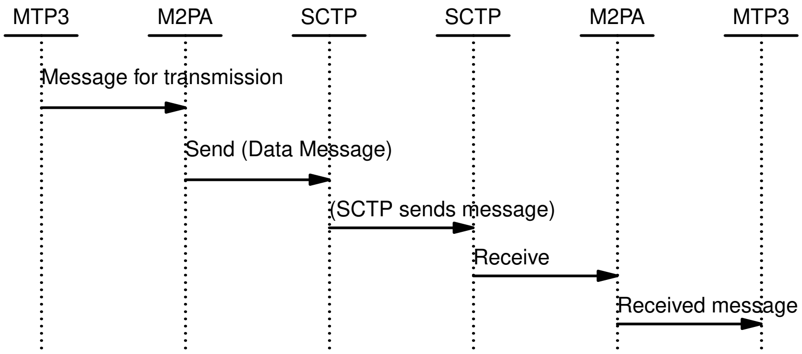

Figure 15. Example: Message Transmission and Reception

5.3. Link Status Indication

If SCTP sends a Communication Lost primitive to M2PA, M2PA notifies MTP3 that the link is out of service. MTP3 responds in its usual way.

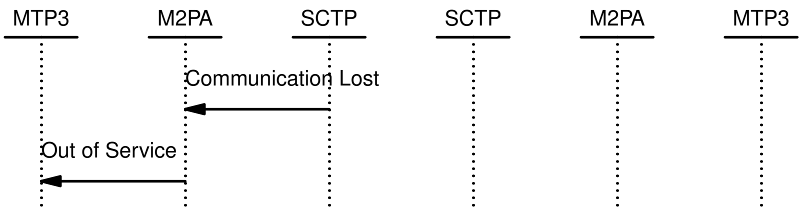

Figure 16. Example: Link Status Indication

5.4. Link Status Message (Processor Outage)

This example shows how M2PA responds to a local processor outage. M2PA sends a Link Status message to its peer. The peer M2PA notifies MTP3 of the outage. MTP3 can then follow the processor outage procedures in Q.703 through Q.704 [Q.703, Q.704].

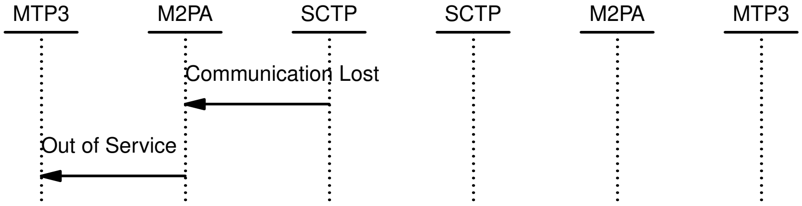

Figure 17. Example: Link Status Message – Processor Outage

5.5. Level 2 Flow Control

This illustrates the Level 2 Flow Control procedure. In the first diagram, congestion ceases before timer T6 expires. The second diagram shows the case where T6 expires.

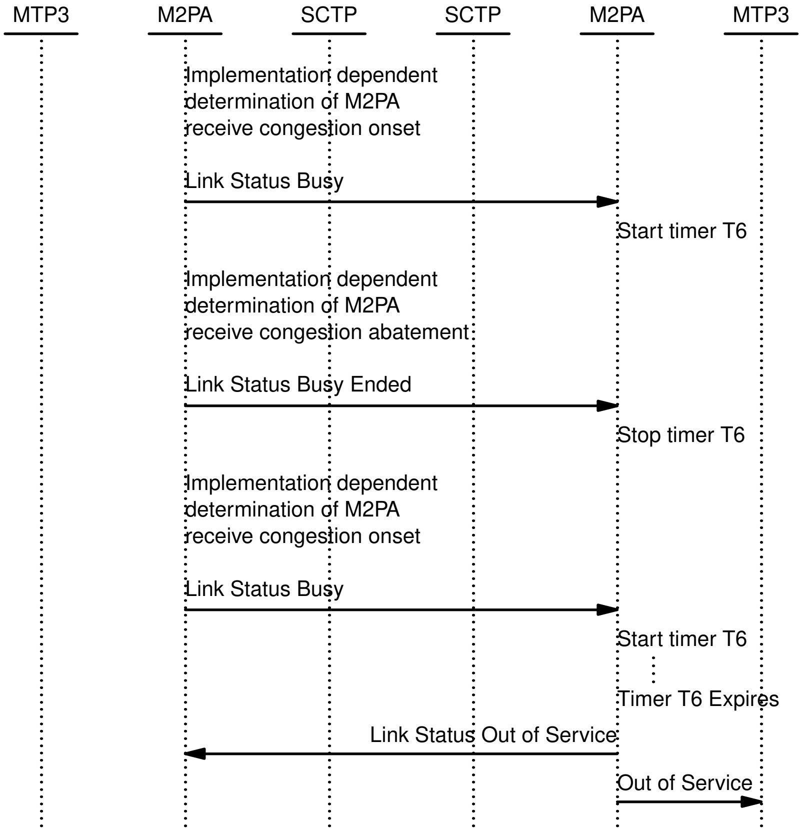

Figure 18. Example: Level 2 Flow Control

5.6. MTP3 Signalling Link Congestion

In this example, M2PA notifies MTP3 of congestion onset and abatement. The notification includes the congestion level, if there are levels of congestion defined.

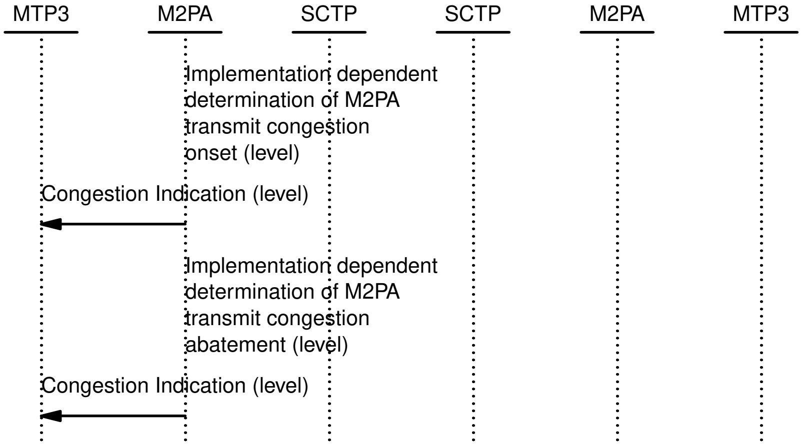

Figure 19. Example: MTP3 Signalling Link Congestion

5.7. Link Deactivation

The MTP3 can request that a SS7-IP link be taken out of service.

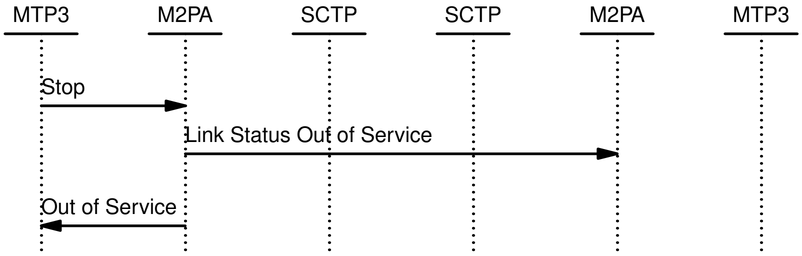

Figure 20. Example: Link Deactivation

5.8. Link Changeover

In this example, MTP3 performs a changeover because the link went out of service. MTP3 selects a different link to retransmit the unacknowledged and unsent messages.

Note that in this example, the sequence numbers and messages requested by MTP3 are sent from SCTP to M2PA in the Communication Lost primitive. In general, the retrieval of sequence numbers and messages is implementation dependent.

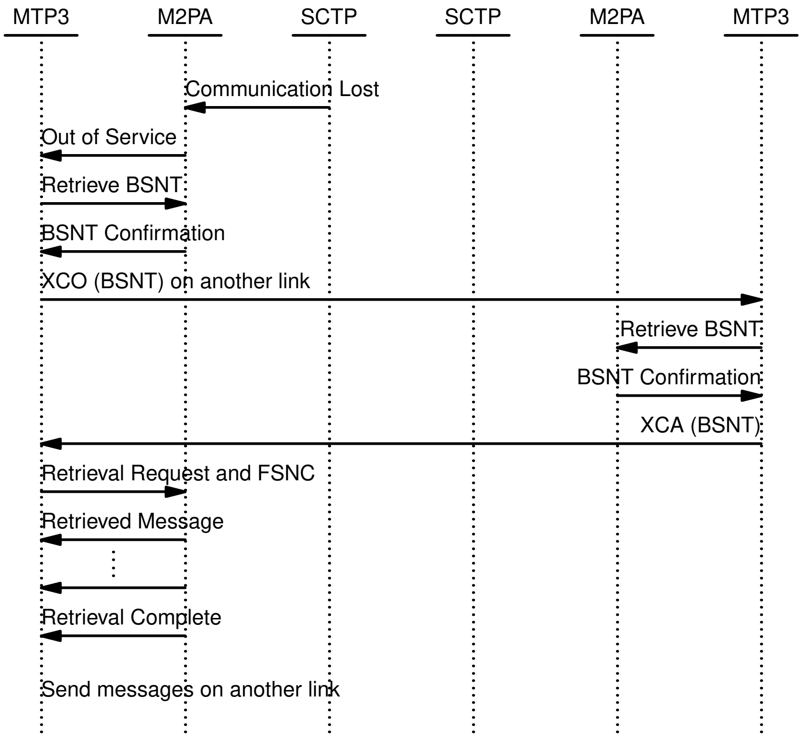

Figure 21. Example: Link Changeover

6. Security

M2PA is designed to carry signalling messages for telephony services. As such, M2PA **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.

6.1. Threats

There is no quick-fix, one-size-fits-all solution for security. As a transport protocol, M2PA has the following security objectives:

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

M2PA runs on top of SCTP. SCTP [RFC 2960] provides certain transport related security features, such as:

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

When M2PA 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" [RFC 2196] **SHOULD** be consulted for guidance.

When the network in which M2PA runs involves more than one party (e.g., a non-private network), 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 be used to ensure confidentiality of user payload. Consult "Security Architecture for the Internet Protocol" [RFC 2401] for more information on configuring IPSEC services.

6.2. 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. IANA Considerations

7.1. SCTP Payload Protocol Identifier

The SCTP (and TCP) Registered User Port Number Assignment for M2PA is 3565.

The value assigned by IANA for the Payload Protocol Identifier in the SCTP Payload Data chunk is

M2PA 5

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.

7.2. M2PA Protocol Extensions

This protocol **MAY** 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 [RFC 2434].

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

7.2.1. IETF Defined Message Classes

The documentation for a new message class **MUST** include the following information:

(a) A long and short name for the message class.

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

7.2.2. IETF Defined Message Types

Documentation of the message type **MUST** contain the following information:

(a) A long and short name for the new message type.

(b) A detailed description of the structure of the message.

(c) A detailed definition and description of the intended use of each field within the message.

(d) A detailed procedural description of the use of the new message type within the operation of the protocol.

(e) A detailed description of error conditions when receiving this message type.

When an implementation receives a message type which it does not support, it **MUST** discard the message.

7.2.3. 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.

(c) Detailed definition of each component of the parameter value.

(d) Detailed description of the intended use of this parameter type, and an indication of whether and under what circumstances multiple instances of this parameter type **MAY** be found within the same message type.

8. Timers

Recommended timer values are as follows:

Table 7. Recommended Timer Values

Timer	(seconds)			
	Range			Default
T1 (Ready)	40	-	50	45
T2 (Not Aligned)	5	-	150	60
T3 (Aligned)	1.0	-	1.5	1.0
T4 (Normal)	7.5	-	9.5	8
T4 (Emerg)	0.400	-	0.600	0.500
T6 (Busy)	3	-	6	4.5
T7 (Ack)	0.5	-	2.0	1.0
Status_Interval	implementation dependent			
Proving_Rate	implementation dependent			

Notes

References

Q.700. ITU, "Introduction to CCITT Signalling System No. 7," ITU-T Recommendation Q.700, ITU-T Telecommunication Standardization Sector of ITU, Geneva (March 1993). [Informative]

Q.703. ITU, "Signalling System No. 7 – Signalling Link," ITU-T Recommendation Q.703, ITU-T Telecommunication Standardization Sector of ITU, Geneva (March 1993). [Normative]

Q.701. ITU, "Functional Description of the Message Transfer Part (MTP) of Signalling System No. 7," ITU-T Recommendation Q.701, ITU-T Telecommunication Standardization Sector of ITU, Geneva (March 1993). [Informative]

Q.702. ITU, "Signalling Data Link," ITU-T Recommendation Q.702, ITU-T Telecommunication Standardization Sector of ITU, Geneva (March 1993). [Informative]

Q.704. ITU, "Message Transfer Part – Signalling Network Functions and Messages," ITU-T Recommendation Q.704, ITU-T Telecommunication Standardization Sector of ITU, Geneva (March 1993). [Normative]

Q.705. ITU, "Signalling System No. 7 – Signalling Network Structure," ITU-T Recommendation Q.705, ITU-T Telecommunication Standardization Sector of ITU, Geneva (March 1993). [Informative]

T1.111.
ANSI, "Signalling System No. 7 – Message Transfer Part," ANSI T1.111, American National Standards Institue (1992). [Normative]

RFC 2719.
L. Ong, I. Rytina, M. Holdrege, L. Coene, M.-A. Garcia, C. Sharp, I. Juhasz, H. P. Lin and HannsJ. Schwarzbauer, "Framework Architecture for Signaling Transport," RFC 2719, The Internet Society (October, 1999). [Informative]

RFC 2960.
R. Stewart, Q. Xie, K. Morneault, C. Sharp, H. J. Schwarzbauer, T. Taylor, I. Rytina, H. Kalla, L. Zhang and V. Paxson, "Stream Control Transmission Protocol (SCTP)," RFC 2960, The Internet Society (February 2000). [Normative]

RFC 791.
, "Internet Protocol – DARPA Internet Program – Protocol Specification," RFC 791, The Internet Society (September 1981). [Normative]

RFC 2119.
S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119 - BCP 14, Internet Engineering Task Force (March 1997). [Normative]

Q.2140.
ITU, "B-ISDN ATM Adaptation Layer – Service Specific Coordination Function for Signalling at the Network

Node Interface (SSCF at NNI)," ITU-T Recommendation Q.2140, ITU-T Telecommunication Standardization Sector of ITU, Geneva (February 1996). [Normative]

Q.2210.
ITU, "Message Transfer Part Level 3 Functions and Messages Using the Services of ITU-T Recommendation Q.2140," ITU-T Recommendation Q.2210, ITU-T Telecommunication Standardization Sector of ITU, Geneva (July 1996). [Normative]

M2UA. K. Morneault, R. Dantu, G. Sidebottom, B. Bidulock and J. Heitz, "Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) - User Adaptation Layer," RFC 3331, Internet Engineering Task Force - Signalling Transport Working Group (September, 2002). [Informative]

JT-Q704.
TTC, "Message Transfer Part – Signalling Network Functions and Messages," TTC Standard JT-Q704, Telecommunication Technology Committee (TTC) (April 28, 1992). [Normative]

RFC 2196.
B. Y. Frazer, "Site Security Handbook," RFC 2196, Internet Engineering Task Force (September 1997). [Normative]

RFC 2401.
S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, Internet Engineering Task Force (November 1998). [Normative]

RFC 2434.
T. Narten, H. T. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs," RFC 2434, The Internet Society (October, 1998). [Normative]

Acknowledgments

The authors would like to thank the following for their valuable comments and suggestions: Brian Tatum, Jeff Copley, Monique Bernard, Wayne Davis, Cliff Thomas, Ian Rytina, Al Varney.

Author's Addresses

Brian Bidulock
OpenSS7 Corporation
1469 Jeffreys Crescent
Edmonton, AB T6L 6T1
Canada
Tel: +1-780-490-1141
Email: bidulock@openss7.org
URL: http//www.openss7.org/

Tom George
Alcatel USA, Inc.
1000 Coit Road
Plano, TX 75075
USA
Tel: +1-972-519-3168
EMail: Tom.George@alcatel.com

Ram Dantu, Ph.D.
Netrake Corporation
3000 Technology Drive, Suite 100
Plano 75074
USA
Tel: +1-214-291-1111
EMail: rdantu@netrake.com

Malleswar Kalla
Telcordia Technologies
MCC 1J211R
445 South Street
Morristown, NJ 07960
USA
Tel: +1-973-829-5212
EMail: kalla@research.telcordia.com

Hanns Juergen Schwarzbauer
SIEMENS AG
Hofmannstr. 51
81359 Munich
Germany
Tel: +49-89-722-24236
HannsJuergen.Schwarzbauer@icn.siemens.de

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

Ken Morneault
Cisco Systems Inc.
13615 Dulles Technology Drive
Herndon, VA 20171
USA
Tel: +1-703-484-3323
EMail: kmorneau@cisco.com

This Internet draft expires July, 2003.

List of Tables

List of Illustrations

Table of Contents

Copyright Statement

Copyright © The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedure for copyrights defined in the Internet Standards process must be followed, or as required to translate into languages other than English.

The limited permission granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and **THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**