Network Working Group
INTERNET-DRAFT
Intended status: PROPOSED STANDARD

Brian Bidulock
OpenSS7 Corporation
June 18, 2007

Expires in December 2007

Signalling Gateway (SG) Information (SGINFO) Support for Signalling User Adaptation Layers

<draft-bidulock-sigtran-sginfo-06.ps>

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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.

This Internet-Draft will expire in December 2007.

Copyright

Copyright © The IETF Trust (2007).

Abstract

This Internet-Draft describes *Signalling Gateway (SG) Information (SGINFO)* for Signalling User Adaptation Protocols [M2UA], [M3UA], [SUA], [ISUA], [TUA], which permits supporting Signalling Gateways (SG) to convey additional Application Server (AS) support information to Application Server Processes (ASPs) activating for AS on the SG. This additional AS support information consists of information pertaining to the underlying SS7 Signalling Provider that otherwise would have to be statically configured at the Application Server Process (ASP) or exchanged between SG and ASP using a non-IETF defined protocol.

Contents

A complete table of contents, list of tables and illustrations, and change history appears at the end of this document.

1. Introduction

1.1. Scope

This Internet-Draft provides parameters and procedures in extension to the parameters and procedures of the Signalling User Adaptation Layers (UAs) [M2UA], [M3UA], [SUA], [ISUA], [TUA], for the purpose of supporting the transfer of SG-specific information of interest to an Application Server during the ASP Active procedure.

UA implementations with *SGINFO* are intended to be compatible with UA implementations not supporting this configuration.

1.2. Abbreviations

AS —Application Server.
ASP —Application Server Process.
IANA —Internet Assigned Numbers Authority
I-D —Internet-Draft
IETF —Internet Engineering Task Force
IP —Internet Protocol.
IPSP —IP Signalling Point.
SCCP —Signalling Connection Control Part.
SCTP —Stream Control Transmission Protocol.
SG —Signalling Gateway.
SGP —Signalling Gateway Process.
SIGTRAN —IETF Signalling Transport WG
SPP —Signalling Peer Process.
SS7 —Signalling System No. 7.
SUA —SS7 SCCP-User Adpatation Layer.
TCAP —Transaction Capabilities Application Part.
TUA —SS7 TCAP-User Adaptation Layer.
UA —User Adaptation Layer.
WG —Working Group

1.3. Terminology

SGINFO adds the following terms to the terminology presented in the UA documents:<1>

Signalling User Adaptation Layer (UA) – one or more of the Stream Control Transmission Protocol (SCTP) [SCTP], [SCTPCRC], [SCTPIG] SS7 Signalling User Adaptation Layers [M2UA], [M3UA], [SUA], [ISUA], [TUA] supporting ASP Management.

1.4. Overview

There is a need to provide extensions for the Signalling User Adaptation Layer protocols to permit a Signalling Gateway (SG) to provide Application Server (AS) specific information pertaining to the SG's ability to support the Application Server.

For example, the "Maximum SIF Length" of MTP3 [Q.704] is a value that an MTP-User at an AS needs to reference to avoid sending MSU data in excess of these MTP-PDU length restrictions. The "Maximum SIF Length"; however, can change due to SS7 Network failures or reconfiguration at the SG that cannot be handled purely by static configuration information at an ASP.

Additional examples exist for SCCP [Q.711] and TCAP [Q.771] and the need for these protocol limits at the Application Server is evidenced by the requirements for these values in the OSI/ISO NSD [X.213] Compliant NPI [NPI], and the OSI/ISO TSD [X.214] and the OSI/ISO ROSE [X.219] Compliant TPI [TPI], and the ACSE [X.217], [X.227] compliant mOSI extensions to the XNS [XNS].

SGINFO provides parameters and procedures that allow Signalling Gateway Processes (SGPs) to inform Application Server Processes (ASPs) of the SG parameters, as well as provides procedures to update these parameters in an active AS.

1.4.1. Existing Information Management

While there is a mandate to provide MIBs to support UA configuration, the existing UA procedures<2> and MIBs make no provisions for the management of dynamic operational information at a Signalling Gateway that is of specific concern to a UA-User at an Application Server (AS).

For example, if an Signalling Gateway changes an operation parameter of necessary to a UA-User at an Application Server (AS), such as the "Maximum SIF Length", there is no mechanism for the SG to communicate this information to the concerned Application Server (AS).

While the existing UA procedures<2> provide for the SG giving an indication of a "Protocol Error" or "Invalid Parameter Value" as a result of an operational parameter being exceeded, there are no procedures for the Application Server to discover the operational parameters when they are dynamic.

The lack of an IETF procedure for managing operational parameter information represents a deficiency of the existing UA procedures<2> that detracts from interoperability between separate implementations of SGP and ASP.

1.4.2. SGINFO Information Management

To remedy these deficiencies, *SGINFO* provides support for the following:

- Support for an SG indicating operational parameters to an Application Server (AS).
- Support for an SG changing operational parameter for an active Application Server (AS).
- Support for interworking between SGPs supporting *SGINFO* and ASPs not supporting *SGINFO*.

Notes for §1

<1> See, for example, Section 1.2 of the specific UA document [M2UA], [M3UA], [SUA], [ISUA], [TUA].

<2> See, for example, Section 4 of the specific UA document [M2UA], [M3UA], [SUA], [ISUA], [TUA].

2. Conventions

The key words "**MUST**", "**MUST NOT**", "**REQUIRED**", "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in [RFC2119].

3. Protocol Elements

SGINFO provides the following parameters and the messages in which they are included in addition to the parameters of the UAs.<1>

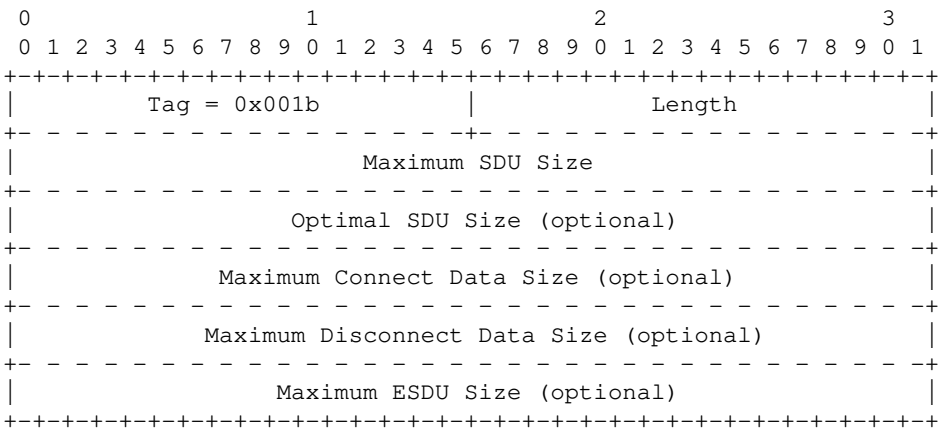
3.1. Parameters

SGINFO provides the following parameters in addition to the parameters defined for the UAs.<1>

3.1.1. Protocol Limits

The *Protocol Limits* parameter is a common parameter used in the **ASPAC ACK** message to indicate the protocol data unit size limitations presented by a Signalling Gateway to an Application Server.

The *Protocol Limits* parameter is formatted as follows:<2>



The *Protocol Limits* parameter contains the following fields:

Maximum SDU Size field: 32-bits (signed integer)

The *Maximum SDU Size* field contains the maximum number of bytes in the *Protocol Data* parameter that the Signalling Gateway can support to the specific Application Server.

M2UA For M2UA [M2UA] the *Maximum SDU Size* field provides the maximum size of the data payload of the *Protocol Data* field. The maximum size is the largest maximum data payload size that can be transferred across the SS7 network by the SG for the specified link. For example, for an SG supporting an SIF Maximum Size [Q.704] of 3094 bytes on the link, this size would be 3094. For an SG supporting 272 bytes, this size would be 272.

M3UA For M3UA [M3UA] the *Maximum SDU Size* field provides the limit on the maximum size of the data payload of the *Protocol Data* field. The maximum size is the largest maximum data payload size that can be transferred across the SS7 network by the SG for the specific Application Server. For example, for an SG supporting both an SIF Maximum Size [Q.704] of 3094 bytes on a primary links and 272 bytes on secondary links, this size would be 3094.

SUA For SUA [SUA] the *Maximum SDU Size* field provides the limit on the maximum size of the User Data field for a normal (non-expedited) data transfer. The maximum size is the largest data payload size that can be transferred across the SS7 network for the specific Application Server (and associated Protocol Class) considering segmentation. If there is no limit on the NSDU size for an SCCP provider at an SG, this field will be set to a value of -1 (0xFFFFFFFF).

TUA For TUA [TUA] the *Maximum SDU Size* field provide the limit on the maximum size of the Components field for a TC-CONTINUE data transfer. The maximum size is the largest component size that can be transferred across the SS7 network for the specific Application Server (and associated Operation Class) considering segmentation. If there is no limit on the component size for a TCAP provider at the SG, this field will be set to a value of -1 (0xFFFFFFFF).

Optimal SDU Size field: 32-bits (signed integer)

The *Optimal SDU Size* field contains the optimal number of bytes in the *Protocol Data* parameter that the Signalling Gateway can support to the specific Application Server.

M2UA For M2UA [M2UA] the *Optimal SDU Size* field does not apply and is not included in the *Protocol Limits* parameter.

M3UA For M3UA [M3UA] the *Optimal SDU Size* field provides the limit on the optimal size of the data payload of the *Protocol Data* field. The optimal size is the smallest maximum data payload size that can be transferred across the SS7 network by the SG for the specific Application Server. For example, for an SG supporting both an SIF Maximum Size [Q.704] of 3094 bytes on a primary links and 272 bytes on secondary links, this size would be 272.

SUA For SUA [SUA] the *Optimal SDU Size* field provides the limit on the optimal size of the User Data field for a normal (non-expedited) data transfer. The optimal size is the largest data protocol size that can be transferred across the SS7 network for the specific Application Server (and associated Protocol Class) without segmentation.

TUA For TUA [TUA] the *Optimal SDU Size* field provides the limit on the optimal size of the Components field for a TC-CONTINUE data transfer. The optimal size is the largest component size that can be transferred across the SS7 network for the specific Application Server (and associated Operation Class) without segmentation.

Maximum Connect Data Size field: 32-bits (signed integer)

The *Maximum Connect Data Size* field contains the maximum number of bytes in the Data parameter that the Signalling Gateway can support to the specific Application Server upon connection or transaction dialogue establishment.

M2UA For M2UA [M2UA] the *Maximum Connect Data Size* field does not apply and is not included in the *Protocol Limits* parameter.

M3UA For M3UA [M3UA] the *Maximum Connect Data Size* field does not apply and is not included in the *Protocol Limits* parameter.

SUA For SUA [SUA] the *Maximum Connect Data Size* field provides a limit on the maximum size of the User Data field that can be included in CORE and COAK messages. For Connection-less operation, this field does not apply and is not included in the *Protocol Limits* parameter.

TUA For TUA [TUA] the *Maximum Connect Data Size* field provides the limit on the maximum size of the User Information and Components that can be included in a TQRY or initial TCNV message. For Operation Class 4, this field does not apply and is not included in the *Protocol Limits* parameter.

Maximum Disconnect Data Size field: 32-bits (signed integer)

The *Maximum Disconnect Data Size* field contains the maximum number of bytes in the Data parameter that the Signalling Gateway can support to the specific Application Server upon disconnection or transaction dialogue abort.

M2UA For M2UA [M2UA] the *Maximum Disconnect Data Size* field does not apply and is not included in the *Protocol Limits* parameter.

M3UA For M3UA [M3UA] the *Maximum Disconnect Data Size* field does not apply and is not included in the *Protocol Limits* parameter.

SUA For SUA [SUA] the *Maximum Disconnect Data Size* field provides a limit on the maximum size of the User Data field that can be included in a RELRE message. For Connection-less operation, this field does not apply and is not included in the *Protocol Limits* parameter.

TUA For TUA [TUA] the *Maximum Disconnect Data Size* field provides the limit on the maximum size of the User Abort Information that can be included in a TUAB message. For Operation Class 4, this field does not apply and is not included in the *Protocol Limits* parameter.

Maximum ESDU Size field: 32-bits (signed integer)

The *Maximum ESDU Size* field contains the maximum number of bytes in the Data parameter that the Signalling Gateway can support to the specific Application Server when data is expedited on a connection.

M2UA For M2UA [M2UA] The *Maximum ESDU Size* field does not apply and is not included in the *Protocol Limits* parameter.

M3UA For M3UA [M3UA] the *Maximum ESDU Size* field does not apply and is not included in the *Protocol Limits* parameter.

SUA For SUA [SUA] the *Maximum ESDU Size* field provides a maximum number of bytes in the User Data field for an expedited data transfer. The maximum size is the largest expedited data payload size that can be transferred across the SS7 network for the specific Application Server. For Connection-less or Protocol Class 2 operation, this field does not apply and is not included in the *Protocol Limits* parameter.

TUA For TUA [TUA] the *Maximum ESDU Size* field does not apply and is not included in the *Protocol Limits* parameter.

3.2. Messages

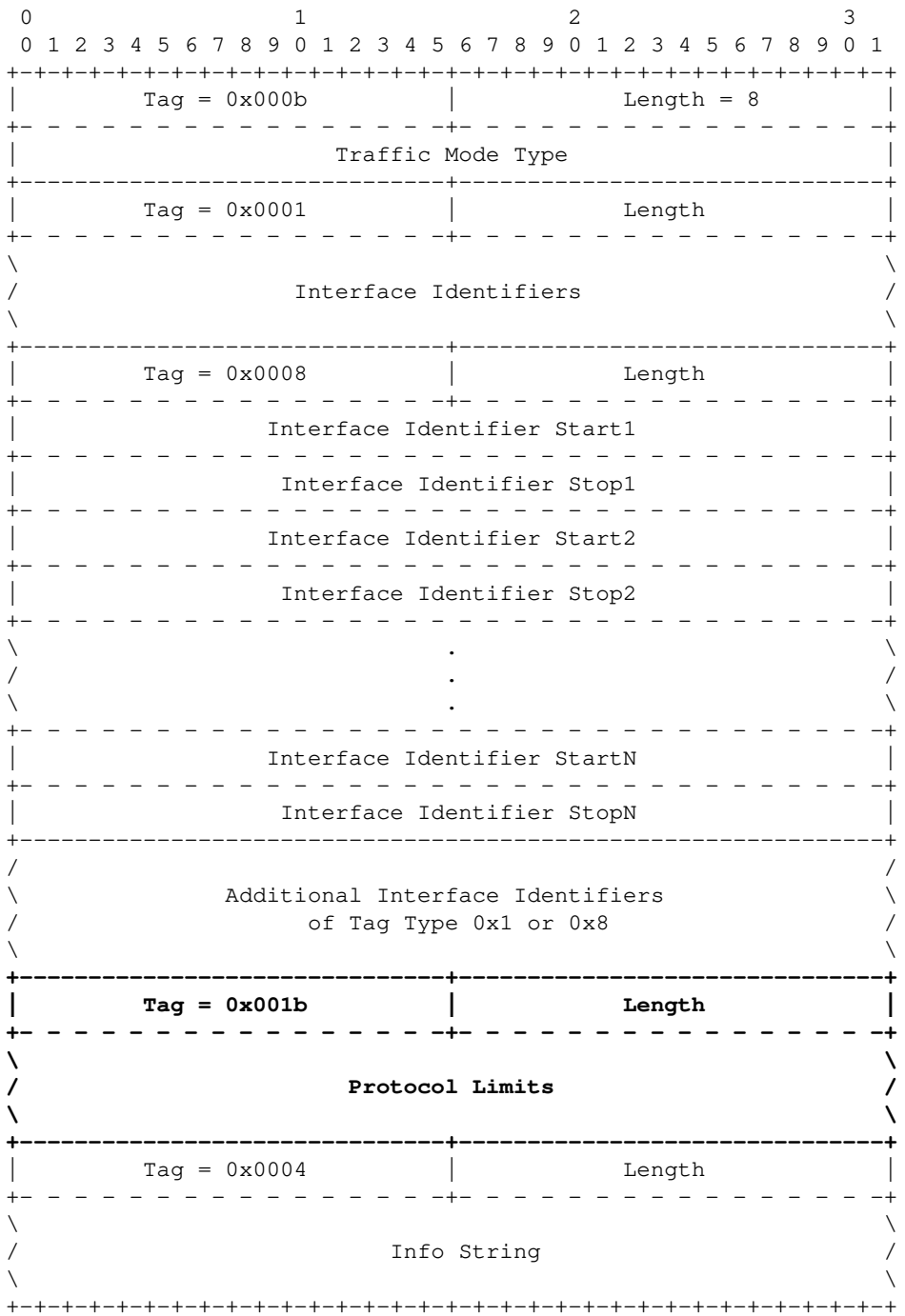
SGINFO extends the following messages defined for the UAs.<1>

3.2.1. ASP Active Acknowledgment (ASPAC ACK)

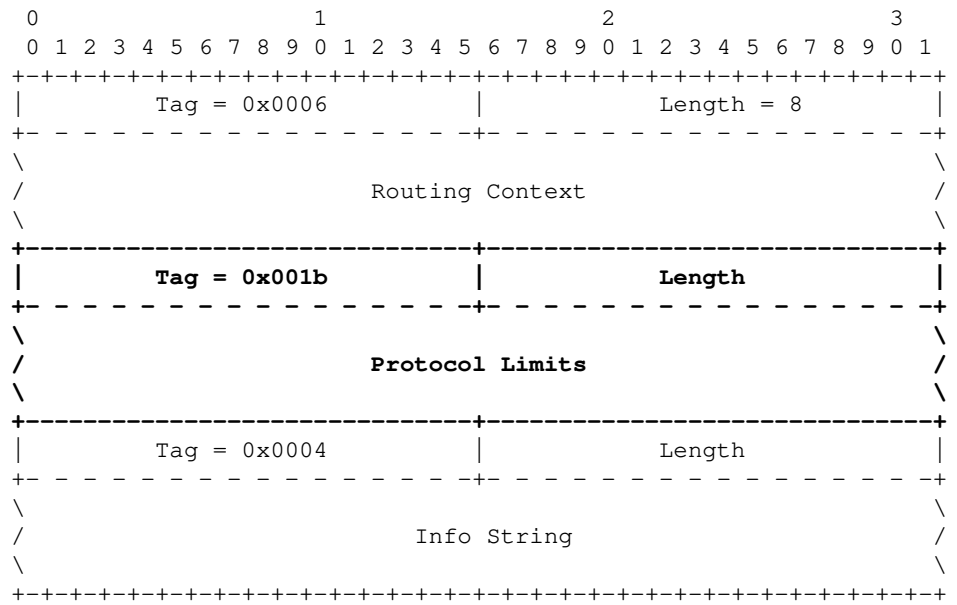
SGINFO supplements the **ASPAC ACK** message by permitting the following optional parameters to be included in the message:

Extension Parameters	
Protocol Limits	Optional

The format of the resulting **ASP ACK** message for M2UA is as follows:<3>



The format of the resulting **ASPAC ACK** message for M3UA, ISUA, SUA and TUA is as follows:<4>



To indicate restrictions on the maximum sizes for transfer of data, the SGP and IPSP **MUST** include the *Protocol Limits* parameter in the **ASPAC ACK** message.

No other changes to the **ASPAC ACK** message format are provided by this extension.

Notes for §3

<1> See, for example, Section 3 of the specific UA document [M2UA], [M3UA], [SUA], [ISUA], [TUA].

<2> **EDITOR'S NOTE:–** The parameter tag values shown as **0x001b** will be assigned by IANA within the common parameter range of the SIGTRAN UAs and may change its value in further versions of this document.

<3> **EDITOR'S NOTE:–** The parameter tag values shown as **0x001b** will be assigned by IANA within the common parameter range of the SIGTRAN UAs and may change its value in further versions of this document.

<4> **EDITOR'S NOTE:–** The parameter tag values shown as **0x001b** will be assigned by IANA within the common parameter range of the SIGTRAN UAs and may change its value in further versions of this document.

4. Procedures

The following procedures are provided in extension to the UA procedures by *SGINFO*.

4.1. ASP Management Procedures

4.1.1. ASP Active Procedures

In extension of the "ASP Active Procedures" of the UAs<2>, *SGINFO* provides the following procedures:

Whenever an SGP, as a part of the normal UA procedures, sends an ASP Active Acknowledgment (ASPAC ACK) to an ASP, it **MAY** include the *Protocol Limits* parameter indicating the protocol data size limits that apply

to the Application Server associated with the *Routing Contexts* (*Interface Identifiers*) specified or implied in the **ASPAC ACK** message. Where the protocol limits only apply to one Application Server, the SGP **SHOULD NOT** include more than one *Routing Context* (*Interface Identifier*) in the **ASPAC ACK** response. That is, in response to an **ASPAC** message containing multiple *Routing Contexts* (*Interface Identifiers*), the SGP **SHOULD** send a separate **ASPAC ACK** reply for each *Routing Context* (*Interface Identifier*) for which it includes the *Protocol Limits* parameter.

If an SG discovers that the protocol data size limits has changed due to an event, (such as a failure in the SS7 network), the SGP **MAY** send an unsolicited **ASPAC ACK** message containing the new protocol limits.

Whenever an ASP receives an **ASPAC ACK** message as part of the normal UA procedures, or receives an unsolicited **ASPAC ACK** for an active Application Server (AS), the ASP will apply the new protocol data size limits to the Application Server.

4.2. Interworking

Whenever an SGP receives an **ERR**("Invalid Parameter") message indicating the *Protocol Limits* parameter in response to a sent **ASPAC ACK** message containing a *Protocol Limits* parameter, the SGP **SHOULD** re-attempt by sending the **ASPAC ACK** without a *Protocol Limits* parameter.

5. Examples

5.1. ASP and SGP both supporting Protocol Limits

An example of an ASP and SGP both supporting Protocol Limits is illustrated in *Figure 1*.

As illustrated in *Figure 1*, the sequence of events for this example are as follows:

(1) An Application Server at an ASP begins in the AS-DOWN or AS-INACTIVE state.

(2) The ASP activates an Application Server by sending an **ASPAC** message.

(3) The SGP responds with an **ASPAC ACK** message containing the current protocol limits in the *Protocol Limits* parameter. The ASP applies these protocol limits to the Application Server upon activation.

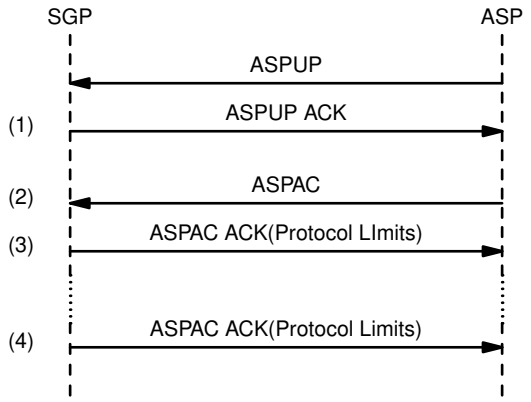


Figure 1. ASP and SGP both supporting Protocol Limits

(4) Later, when the SGP notes a change to protocol limits, the SGP sends an unsolicited **ASPAC ACK** message containing the updated *Protocol Limits*. The ASP applies these updated protocol limits to the Application Server upon receipt.

5.2. SGP only supporting Protocol Limits

5.2.1. ASP ignores Protocol Limits

An example of an SGP only supporting Protocol Limits where the ASP ignores the *Protocol Limits* parameter is illustrated in *Figure 2*.

As illustrated in *Figure 2*, the sequence of events for this example are as follows:

(1) An Application Server at an ASP begins in the AS-DOWN or AS-INACTIVE state.

(2) The ASP activates an Application Server by sending an **ASPAC** message.

(3) The SGP responds with an **ASPAC ACK** message containing the current protocol limits in the *Protocol Limits* parameter. The ASP ignores the *Protocol Limits* parameter and, instead, relies upon internal configuration data to determine protocol limits.

(4) Later, when the SGP notes a change to protocol limits, the SGP sends an unsolicited **ASPAC ACK** message containing the updated *Protocol Limits*. The ASP ignores the *Protocol Limits* parameter and, instead, relies upon internal configuration data to determine protocol limits.

5.2.2. ASP refuses Protocol Limits

An example of an SGP only supporting Protocol Limits where the ASP refuses the *Protocol Limits* parameter is illustrated in *Figure 3*.

As illustrated in *Figure 3*, the sequence of events for this example are as follows:

(1) An Application Server at an ASP begins in the AS-DOWN or AS-INACTIVE state.

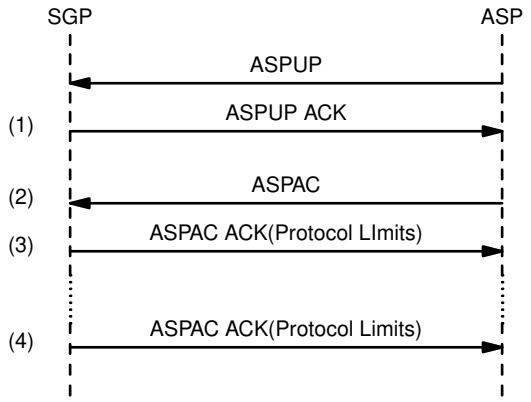


Figure 2. ASP and SGP both supporting Protocol Limits

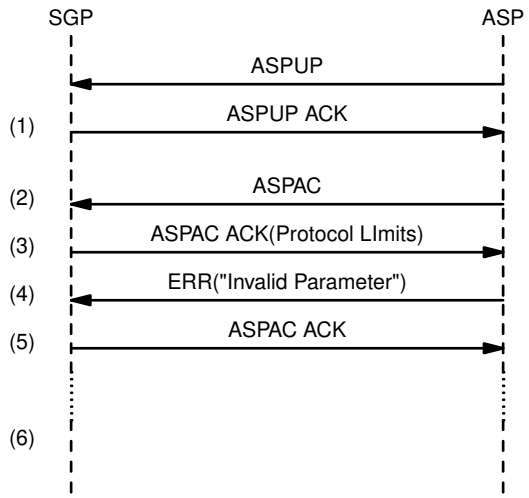


Figure 3. ASP and SGP both supporting Protocol Limits

(2) The ASP activates an Application Server by sending an **ASPAC** message.

(3) The SGP responds with an **ASPAC ACK** message containing the current protocol limits in the *Protocol Limits* parameter.

(4) The ASP refuses the **ASPAC ACK** message and responds with an **ERR**("Invalid Parameter") message indicating the *Protocol Limits* parameter as invalid.

(5) The SGP re-attempts and sends the **ASPAC ACK** message without the *Protocol Limits* parameter and marks the ASP as incapable of processing protocol limits.

(6) When a subsequent change in the protocol limits at the SGP occurs, the SGP does nothing (the ASP is marked as incapable of handling protocol limits).

5.3. ASP only supporting Protocol Limits

An example of an ASP only supporting Protocol Limits is illustrated in *Figure 4*.

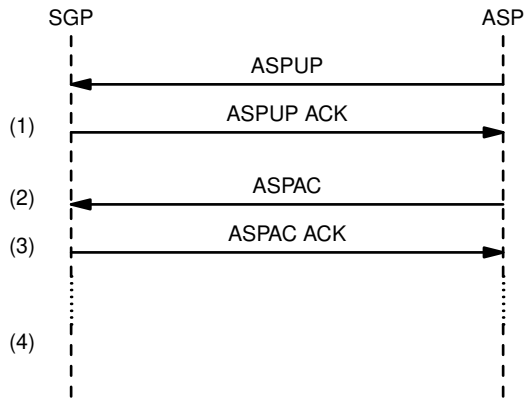


Figure 4. ASP and SGP both supporting Protocol Limits

As illustrated in *Figure 4*, the sequence of events for this example are as follows:

(1) An Application Server at an ASP begins in the AS-DOWN or AS-INACTIVE state.

(2) The ASP activates an Application Server by sending an **ASPAC** message.

(3) The SGP responds with an **ASPAC ACK** message not containing the *Protocol Limits* parameter.

(4) The ASP receiving the **ASPAC ACK** with no *Protocol Limits* parameter relies upon internal configuration data to determine protocol limits.

6. Security

SGINFO does not introduce any new security risks or considerations that are not already inherent in the UA [M2UA], [M3UA], [SUA], [ISUA], [TUA] Please see the SIGTRAN Security document [SIGSEC] for security considerations and recommendations that are applicable to each of these UAs.

7. IANA Considerations

7.1. Protocol Extensions

SGINFO provides an additional *Protocol Limits* message parameter to the common parameter range of the SIGTRAN UAs [M2UA], [M3UA], [SUA], [ISUA], [TUA]:

(a) The parameter is named the *Protocol Limits* parameter.

(b) The structure of the *Protocol Limits* parameter field conforms to the UA general TLV format and is described in detail in Section 3.1.1.

(c) The detailed definition of each component of the *Protocol Limits* parameter values is described in Section 3.1.1.

(d) This document also provides a detailed description of the intended use of the *Protocol Limits*<1> parameter, and in which messages the *Protocol Limits* parameter should appear, how many times, and when.

Notes for §7

<1> **EDITOR'S NOTE:–** The *Protocol Limits* parameter tag value shown throughout this document as **`0x001b`** will be assigned by IANA within the common parameter range of the SIGTRAN UAs and may change its value in further versions of this document.

0. Revision History

This section provides historical information on the changes made to this draft. This section will be removed from the document when the document is finalized.

0.6. Changes from Version 0.5 to Version 0.6

- updated new boilerplate and idnits 2.00.1.
- updated references, version numbers and dates.

0.5. Changes from Version 0.4 to Version 0.5

- updated to IETF boilerplate for first and last page.
- updated references, version numbers and dates.
- resubmitted to sync with IETF numbering

0.4. Changes from Version 0.3 to Version 0.4

- updated references, version numbers and dates.

0.3. Changes from Version 0.2 to Version 0.3

- added list of abbreviations.
- moved history section.
- updated revision and dates.
- updated references.
- split reference section.
- updated secuirty section.
- moved notes to end.

0.2. Changes from Version 0.1 to Version 0.2

- added this section,
- updated references, release version and dates,
- minor corrections,
- updated postscript diagrams,
- updated author's address.

0.1. Changes from Version 0.0 to Version 0.1

0.0. Version 0.0

0.0.0. Change Log

```
$Log: draft-bidulock-sigtran-sginfo-06.me,v $
Revision 0.9.2.1  2007/02/03 15:47:25  brian
- added new drafts

Revision 0.9.2.5  2006/06/27 09:41:15  brian
- rereleased drafts

Revision 0.9.2.4  2006/06/18 20:53:35  brian
- preparing for draft rerelease

Revision 0.9.2.3  2005/10/17 11:53:46  brian
- updated drafts for republication

Revision 0.9.2.2  2005/05/14 08:33:21  brian
- copyright header correction

Revision 0.9.2.1  2004/03/16 05:10:46  brian
- Added drafts and figures.

Revision 0.8.2.1  2003/08/01 12:23:16  brian
Added abbreviations, updated format.
```

Normative References

[**RFC2119**] Bradner, S., *"Key words for use in RFCs to Indicate Requirement Levels,"* **BCP 14/RFC 2119**, The Internet Society (March 1997). **<http://www.ietf.org/rfc/rfc2119.txt>**

[**M2UA**] Morneault, K., Dantu, R., Sidebottom, G., Bidulock, B. and Heitz, J., *"Signaling System 7 (SS7) Message Transfer Part 2 (MTP2) — User Adaptation Layer,"* **RFC 3331**, The Internet Society (September 2002). **<http://www.ietf.org/rfc/rfc3331.txt>**

[**M3UA**] Morneault, K., Pastor-Balbas, J., (eds), *"Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) — User Adaptation Layer (M3UA),"* **RFC 4666**, The Internet Society (September 2006). **<http://www.ietf.org/rfc/rfc4666.txt>**

[**SUA**] Loughney, J., Sidebottom, G., Coene, L., Verwimp, G., Keller, J. and Bidulock, B., *"Signalling Connection Control Part User Adaptation Layer (SUA),"* **RFC 3868**, The Internet Society (October 2004). **<http://www.ietf.org/rfc/rfc3868.txt>**

[**SCTP**] Stewart, R. R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H. J., Taylor, T., Rytina, I., Kalla, H., Zhang, L. and Paxson, V., *"Stream Control Transmission Protocol (SCTP),"* **RFC 2960**, The Internet Society (October 2000). *(Updated by RFC 3309) (Status: PROPOSED STANDARD)* **<http://www.ietf.org/rfc/rfc2960.txt>**

[**SCTPCRC**] Stone, J., Stewart, R. R. and Otis, D., *"Stream Control Transmission Protocol (SCTP) Checksum Change,"* **RFC 3309**, The Internet Society (September 2002). *(Updates RFC 2960) (Status: PROPOSED STANDARD)* **<http://www.ietf.org/rfc/rfc3309.txt>**

[**SIGSEC**] Loughney, J., Tuexen, M. and Pastor-Balbas, J., *"Security Considerations for Signaling Transport (SIGTRAN) Protocols,"* **RFC 3788**, Internet Engineering Task Force — Signalling Transport Working Group (June 2004). **<http://www.ietf.org/rfc/rfc3788.txt>**

Informative References

[**ISUA**] Bidulock, B., *"SS7 ISUP-User Adaptation Layer (ISUA),"* **draft-bidulock-sigtran-isua-04.txt**, Internet Engineering Task Force — Signalling Transport Working Group (February 3, 2007). *Work In Progress.* **<http://www.ietf.org/internet-drafts/draft-bidulock-sigtran-isua-04.txt>**

[**TUA**] Bidulock, B., *"SS7 TCAP-User Adaptation Layer (TUA),"* **draft-bidulock-sigtran-tua-05.txt**, Internet Engineering Task Force — Signalling Transport Working Group (February 3, 2007). *Work In Progress.* **<http://www.ietf.org/internet-drafts/draft-bidulock-sigtran-tua-05.txt>**

[**SCTPIG**] Stewart, R., Aria-Rodriguez, I., Poon, K., Caro, A. and Tuexen, M., *"Stream Control Transmission Protocol (SCTP) Specification Errata and Issues,"* **RFC 4460**, The Internet Society (April 2006). *(Status: INFORMATIONAL)* **<http://www.ietf.org/rfc/rfc4460.txt>**

[**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). *(Previously "CCITT Recommendation")*

[**Q.711**] ITU, *"Functional Description of Signalling Connection Control Part,"* **ITU-T Recommendation Q.711**, ITU-T Telecommunication Standardization Sector of ITU, Geneva (March 1993). *(Previously "CCITT Recommendation")*

[**Q.771**] ITU, *"Signalling System No. 7 — Functional Description of Transaction Capabilities,"* **ITU-T Recommendation Q.771**, ITU-T Telecommunication Standardization Sector of ITU, Geneva (March 1993). *(Previously "CCITT Recommendation")*

[**X.213**] ITU, *"OSI — Network Service Definition,"* **ITU-T Recommendation X.213 [ISO/IEC 8348]**, ITU-T Telecommunication Standardization Sector of ITU, International Organization for Standardization, Geneva (November 1995). *(Previously "CCITT Recommendation")*

[**NPI**] UNIX International, Inc., *"Network Provider Interface (NPI) Specification,"* **NPI Revision 2.0.0**, UNIX International Press, Parsippany, New Jersey (August 17, 1992). **<http://www.openss7.org/docs/npi.pdf>**

[**X.214**] ITU, *"Information Technology — Open Systems Interconnection — Transport service definition,"* **ITU-T Recommendation X.214 [ISO/IEC 8072 : 1996]**, ITU-T Telecommunication Standardization Sector of ITU, International Organization for Standardization, Geneva (November 1995). *(Previously "CCITT Recommendation")*

[**X.219**] ITU, *"Information processing systems — Text Communication, Remote Operations: Model, Notation and Service Definition,"* **ITU-T Recommendation X.219 [ISO/IEC 9072-1]**, ITU-T Telecommunication Standardization Sector of ITU, International Organization for Standardization, Geneva (n.d.). *(Previously "CCITT Recommendation")*

[**TPI**] Open Group, *"Transport Provider Interface (TPI) Specification,"* **TPI Revision 2.0.0**, Open Group Publication, Parsippany, New Jersey (1999). **<http://www.opengroup.org/onlinepubs/>**

[**X.217**] ITU, *"Information Technology — Open Systems Interconnection — Service definition for the Association Control Service Element,"* **ITU-T Recommendation X.217 [ISO/IEC 8649 : 1996]**, ITU-T Telecommunication Standardization Sector of ITU, International Organization for Standardization, Geneva (1995). *(Previously "CCITT Recommendation")*

[**X.227**] ITU, *"Information Technology — Open Systems Interconnection — Connection-oriented protocol for the Association Control Service Element: Protocol Specification,"* **ITU-T Recommendation X.227 [ISO/IEC 8650-1]**, ITU-T Telecommunication Standardization Sector of ITU, International Organization for Standarization, Geneva (1995). *(Previously "CCITT Recommendation")*

[**XNS**] Open Group, *"Technical Standard: Network Services (XNS),"* **XNS Issue 5.2 Draft 2.0** [ISBN 1-85912-241-8], Open Group Publication (1999). **<http://www.opengroup.org/onlinepubs/>**

Author's Addresses

Brian Bidulock
OpenSS7 Corporation
1469 Jeffreys Crescent
Edmonton, AB T6L 6T1
Canada

Phone: +1-780-490-1141
Email: bidulock@openss7.org
URL: http//www.openss7.org/

This draft expires December 2007.

List of Illustrations

Figure 1. ASP and SGP both supporting Protocol Limits 9
Figure 2. ASP and SGP both supporting Protocol Limits 10
Figure 3. ASP and SGP both supporting Protocol Limits 11
Figure 4. ASP and SGP both supporting Protocol Limits 11

Table of Contents

Status of this Memo 1
Copyright 1
Abstract 1
Contents 1
1 Introduction 1
1.1 Scope 1
1.2 Abbreviations 2
1.3 Terminology 2
1.4 Overview 2
1.4.1 Existing Information Management 2
1.4.2 SGINFO Information Management 3
Notes for §1 3
2 Conventions 3
3 Protocol Elements 3
3.1 Parameters 3
3.1.1 Protocol Limits 3
3.2 Messages 6
3.2.1 ASP Active Acknowledgment (ASPAC ACK) 6
Notes for §3 8
4 Procedures 8
4.1 ASP Management Procedures 8
4.1.1 ASP Active Procedures 8
4.2 Interworking 9
5 Examples 9
5.1 ASP and SGP both supporting Protocol Limits 9
5.2 SGP only supporting Protocol Limits 10
5.2.1 ASP ignores Protocol Limits 10
5.2.2 ASP refuses Protocol Limits 10
5.3 ASP only supporting Protocol Limits 11
6 Security 12
7 IANA Considerations 12
7.1 Protocol Extensions 12
Notes for §7 12
0 Revision History 13
0.6 Changes from Version 0.5 to Version 0.6 13
0.5 Changes from Version 0.4 to Version 0.5 13

0.4 Changes from Version 0.3 to Version 0.4 13
0.3 Changes from Version 0.2 to Version 0.3 13
0.2 Changes from Version 0.1 to Version 0.2 13
0.1 Changes from Version 0.0 to Version 0.1 13
0.0 Version 0.0 14
0.0.0 Change Log 14
Normative References 15
Informative References 15
Author's Addresses 17
List of Illustrations 18
Table of Contents 18

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and **THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.**

Full Copyright Statement

Copyright © The IETF Trust (2007). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.