Oracle® Communications Network Charging and Control

SIGTRAN sua_if Protocol Implementation Conformance Statement

Release 12.0.0

December 2017

ORACLE®

Copyright

Contents

About This Document

Scope

This document describes the extent to which the Oracle sua_if conforms with RFC 3868 “Signalling Connection Control Part User Adaptation Layer (SUA)”.

Audience

This document is intended for Oracle and customer staff familiar with the sua_if program and the SUA protocol.

References

- [RFC 3868] RFC 3868. Signalling Connection Control Part User Adaptation Layer (SUA). J. Loughney, Ed., G. Sidebottom, L. Coene, G. Verwimp, J. Keller, B. Bidulock. October 2004.
- [SUA GUIDE] draftietfsigtransuaimplementorguide03.txt. L. Coene, J. Loughney. IETF Internet Draft. March 2006.

Revision history

Here are the changes to the document.

Version no.	Revision Date	Description
0.1	2006-08-10	Initial Version
0.2	2006-08-29	Update for recent changes.
1.1	2007-10-09	Clarify subsection coverage. Bring up to date.
1.2	2008-01-25	Update for Sigtran 1.2 release
03.00	2010-10-08	Re-format to standard.
04.00	2010-11-11	Re-branded & published

Document Conventions

Format

Section numbers within RFC 3868 are reused within this document. Section numbers from RFC 3868 are omitted if no comment is needed.

Terminology

The word “compliant” in this document means that the sua_if program behaves in a manner compatible with the relevant requirements of the RFC 3868 text (as updated by [SUA GUIDE]).

The words “implemented” or “supported” in this document specifies what parts of the RFC 3868 text are supported by the sua_if program. Implemented behavior may also be described without explicit use of the words “implemented” or “supported”.

In some cases, “compliant” and “implemented” are orthogonal. Compliance does not necessarily imply the implementation of functionality in RFC 3868 that is optional or not applicable.

Implemented does not imply compliance, although noncompliance of implemented behavior is always noted.

Where a configurable sua_if parameter is involved in compliance to a requirement, it is assumed that the configuration meets that requirement. Configuring a parameter to an illegal value may silently cause the sua_if program to operate in a non-compliant manner.

The IETF internet draft [SUA GUIDE] contains corrections and minor modifications to RFC 3868.

These changes are noted where relevant to the compliance or implementation of the sua_if program.

Chapter 1

SIGTRAN sua_if PICS

Overview

Introduction

This chapter describes the extent to which the Oracle sua_if conforms with RFC 3868 “Signalling Connection Control Part User Adaptation Layer (SUA)”.

In this chapter

This chapter contains the following topics.

1. [RFC 3868] Introduction

Introduction

The sua_if program transports TCAP (both ANSI and ITU variants) over SUA.

1.1 Scope

The sua_if program is an IP signalling endpoint. It may connect to either signalling gateways or other IP signalling endpoints.

1.2 Abbreviations and Terminology

Compliant.

1.3 Signalling Transport Architecture

1.3.1. Protocol Architecture for Connectionless Transport

Connectionless transport is supported.

1.3.2. Protocol Architecture for Connection-Oriented Transport

Connection-orientated transport is not supported.

1.3.3. All IP Architecture

The sua_if supports an all IP network architecture.

1.3.4. ASP Fail-over Model and Terminology

The sua_if supports failover.

1.4. Services Provided by the SUA Layer

Section 1.4 and sub-sections are compliant except as noted below.

1.4.1. Support for the transport of SCCP-User Messages

The sua_if supports the transfer of SCCPuser messages.

1.4.2. SCCP Protocol Class Support

Only protocol classes 0 and 1 are supported.

1.4.3 Native Management Functions

Compliant.

1.4.4 Interworking with SCCP Network Management Functions

Non-compliant as sua_if, in itself, is not a signaling gateway and does not interact with SCCP.

1.4.5 Support for the Management Between the SGP and ASP

Non-compliant as sua_if, in itself, is not a signaling gateway and does not interact with SCCP.

1.4.6 Relay Functionality

The sua_if does not support relay functionality.

1.5. Internal Functions Provided in the SUA Layer

Routing information is loaded from a configuration file, using the standard Oracle eserv.config file format.

1.5.1. Address Mapping at the SG

The sua_if performs address mapping based on various fields in both the destination and source addresses:

- Point-code,
- Global-title digits (destination address only),
- Routing-indicator,
- Address-indicator,
- Sub-system number,
- GTI,
- Translation type,
- Number plan,
- Nature-of-address.

Buffering using T(r) is not implemented.

Note: Although sua_if implements an AS(P), some SG functionality is relevant for an all-IP architecture where the sua_if is connected directly to another AS(P).

1.5.2. Address Mapping at the ASP

The sua_if performs address mapping based on various fields in both the destination and source addresses, as listed in 1.5.1 above.

1.5.3. Address Mapping Function at a Relay Node

Not applicable. The sua_if does not provide relation functionality.

1.5.4. SCTP Stream Mapping

Compliant.

The sua_if uses unordered delivery for data packets (CLDT) with an even protocol class (e.g., qos values 0 and 0x80) and ordered delivery for all other packets.

If only stream 0 is available, that is used for all traffic.

If multiple streams are available, stream 0 is not used for data traffic.

1.5.5. Flow Control

The sua_if does not implement flow control beyond that provided by the underlying SCTP layer.

1.5.6. Congestion Management

Congestion notifications are not generated.

1.6. Definition of SUA Boundaries

Note that as the sua_if program includes the upper layer userpart above SCCP, the notions defined in 1.6 are not visible outside of the sua_if program and are not relevant to this document.

In fact, in many places, the implementation of the sua_if program does not follow the design that one may infer to be suggested by RFC 3868.

2. Conventions

Nothing to comply to.

3. Protocol Elements

Introduction

Section 3 and subsections are compliant except as noted otherwise.

Note that compliance in section 3 in general only covers packet formatting and does not indicate any particular level of compliance with the procedures using those packets.

The sua_if packet code can recognize all RFC 3868 packets and parameters.

However, certain packets and fields in incoming traffic may be ignored, and certain packets and fields may not be generated on outgoing packets.

For such unused packets and fields, compliance in this section merely means that the error (if any) generated on receipt indicates lack-of-support rather than an invalid packet.

3.1. Common Message Header

3.1.1 SUA Protocol Version

Compliant.

3.1.2 Message Classes

Compliant.

3.1.3 Message Types

Compliant.

3.1.4. Message Length

There is a limit of 8192 bytes for incoming SUA packets.

3.1.5. Tag-Length-Value Format

Parameters within a packet are sent in the order in which they appear in RFC 3868.

Parameters within a received packet may be in any order.

3.2. SUA Connectionless Messages

Compliant.

3.3. Connection Orientated Messages

Compliant, although connection orientated messages are not used by the sua_if. If received, an appropriate Error packet will be returned.

3.4. Signalling Network Management (SNM) Messages

Compliant. Although DAUD messages are not responded to.

3.5. Application Server Process State Maintenance Messages

3.5.1. ASP Up (UP)

Compliant.

3.5.2. ASP Up Ack (UP ACK)

Compliant.

3.5.3. ASP Down (DOWN)

Compliant.

3.5.4. ASP Down Ack (DOWN ACK)

Compliant.

3.5.5. Heartbeat (BEAT)

Compliant. BEAT messages are not sent (instead, SCTP heartbeats are enabled if configured).

BEAT messages are responded to.

3.6. ASP Traffic Maintenance Messages

Compliant.

3.7. SUA Management Messages

3.7.1. Error (ERR)

Compliant.

Error messages are not generated in response to invalid Error messages, as per [SUA GUIDE].

3.7.2. Notify (NTFY)

3.8. Routing Key Management (RKM) Messages.

Routing Key Management messages are not supported by sua_if and an Error is returned on receipt.

Compliant in so far as that is meaningful.

3.9. Common Parameters

Compliant.

3.9.1. Not Used

Use of parameter in SUA messages is not supported.

3.9.2. Not Used

Use of parameter in SUA messages is not supported.

3.9.3. Not Used

Use of parameter in SUA messages is not supported.

3.9.4. Info String

3.9.5. Not Used

Use of parameter in SUA messages is not supported.

3.9.6. Routing Context

Compliant. Following [SUA GUIDE], the Routing Context parameter is an array of 32-bit values in some contexts, and a single 32-bit value in others. There are some limitations in the routing context handling; see 4.3.1 and 4.3.2 below for details.

3.9.7. Diagnostic Information

3.9.8. Not Used

Use of parameter in SUA messages is not supported.

3.9.9. Heartbeat Data

3.9.10. Not Used

Use of parameter in SUA messages is not supported.

3.9.11 Traffic Mode Type

3.9.12. Error Code

Compliant. The “Invalid Network Appearance” and “Invalid Routing Context” errors are not generated, so the two occurrences of “MUST” in the text are null requirements

3.10. SUA-Specific Parameters

3.10.1. SS7 Hop Counter

3.10.2. Source Address

Only SSN/GT/PC addresses are supported by the sua_if. Other address fields will be ignored.

3.10.2.1. Routing Indicator

3.10.2.2. Address Indicator

3.10.2.3. Global Title

As per [SUA GUIDE], filler bytes are not included in the parameter length.

4. Procedures

4.1. Procedures to Support the SUA-User Layer

4.1.1. Receipt of Primitives from SCCP

Compliant. The only relevant item is the SCTP stream selection.

4.2. Receipt of Primitives from the Layer Management

4.2.1. Receipt of SUA Peer Management Messages

Non-data messages are always sent on SCTP stream 0.

4.3. AS and ASP State Maintenance

Compliant with section 4.3 and subsections, except as noted below. Details of implementation follow.

Both the “Single Exchange” and “Double Exchange” models are supported. For the asymmetric SE model, the sua_if program supports operation as either end of the connection. There are some limitations in situations where the sua_if program is pretending to be a SGP end-point.

It’s not clear from the specification whether the DE model requires the two state machines to run in lock-step (i.e., both go up then both go active), or whether the two state machines run independently (i.e., one end may go active even before the other end goes up). We implement the latter.

4.3.1. ASP States

Compliant. Messages are not sent to DOWN or INACTIVE ASPs as recommended.

When shutting down a connection, timeouts are applied, and the SCTP connection will be closed without completing the inactive/down interaction if a timeout expires.

The timeout is 2 seconds for each expected response packet.

The sua_if program supports only one AS per local ASP. In other words, ACTIVE packets will only ever be sent for one routing context per SCTP connection. A peer ASP may activate any number of routing contexts.

The routing context actually used is (a) the routingcontext of the local ASP, if active, else (b) the first routing context activated by the remote ASP.

4.3.2. AS States

Compliant (including 4.3.2.1).

A non-override ASP is activated based on received NTFY packets; other ASPs are activated immediately on reaching UP.

4.3.3. SUA Management Procedures for Primitives

Compliant.

When configured to make an outbound SCTP connection, the sua_if will attempt a reconnect 5 seconds after the connection is disconnected (or after a previous unsuccessful connection attempt).

4.3.4. ASPM Procedures for Peer-to-Peer Messages

4.3.4.1. ASP Up Procedures

Compliant (including subsections).

See above for some details and behaviour.

4.3.4.2. ASP Down Procedures

Compliant.

4.3.4.3. ASP Active Procedures

For sending Active packets, we only support a single routing context per connection.

When receiving Active packets, we accept any routing contexts. We do not enforce any particular routing context values; we allow a remote ASP to use any routing context value whatsoever.

We send a single Active Ack message per received Active message.

4.3.4.4. ASP Inactive Procedures

The sua_if program does not buffer packets using the T(r) timer. The appropriate NTFY packets are however generated using the timer.

4.3.4.5. Notify Procedures

Compliant.

4.3.4.6. Heartbeat procedures

Compliant. We respond to incoming heartbeat packets. We do not sent heartbeat packets; instead SCTP heartbeats are used.

4.4. Routing Key Management Procedures

Section 4.4 and subsections are not supported.

On receiving a RKM packet, we respond with an “Unsupported message class” error. (RFC3868 states unsupported message type; this is changed to unsupported message class in [SUA GUIDE]).

4.5. Availability and/or Congestion Status of SS7 Destination Support

4.5.1. At an SGP

The sua_if program is not an SGP.

4.5.2. At an ASP

Compliant (including subsections) in that SSNM messages are notified to layer management as required. However, the RFC does not specify processing beyond that, so compliance here is more-or-less meaningless. The sua_if layer management ignores SSNM messages except for logging them appropriately.

4.5.3. ASP Auditing

The sua_if program does not send or respond to DAUD messages.

4.6. MTP3 Restart

The sua_if program does not handle MTP3 over SS7 connections.

4.7. SCCP – SUA Interworking at the SG

4.7.1. Segmenting / Reassembly

Compliant.

4.7.2. Support for Loadsharing

Compliant.

The sua_if program supports two slightly different loadsharing mechanisms for outbound traffic:

1 By configuring a set of PCs as STPs to relay other traffic.
2 By routing a PC or GT to multiple destinations.

Mechanism 1 correctly supports TCAP loadshare.

Mechanism 2 loadshares based on SLS; the mapping of SLS values to connections may change when connections are (de)activated.

4.7.3. Routing and message distribution at the SG

4.7.3.1. TCAP traffic

Compliant, but see the caveat in 4.7.2.

4.7.4. Multiple SGs, SUA Relay Function

The sua_if program is not an SG and does not act as a relay.

5. Examples of SUA Procedures

Introduction

This section (and subsections) do not state requirements for compliance.

6. Security Considerations

Introduction

This section (and subsections) do not state requirements for compliance.

7. IANA Considerations

7.1. SCTP Payload Protocol ID

Compliant. The PPID value 4 is always used.

7.2. Port Number

Compliant. The port numbers are configurable and 14001 may be used.

7.3. Protocol Extensions

This section (including subsections) does not place requirements upon an implementation. No extensions are supported.

8. Timer Values

Introduction

T(r) is hardwired to 2 seconds.

T(ack) is hardwired to 2 seconds.

Failed connections are retried every 5 seconds, when acting as the client end of the SCTP connection.

Other timer values are not relevant.

Appendix A.

Appendix A does not place requirements upon an implementation. See the rest of this document for details of what is reported.

Index

1

2

3

4