Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: January 22, 2015

P. Dawes
Vodafone Group

July 21, 2014

Requirements for Marking SIP Messages to be Logged
draft-ietf-insipid-logme-reqs-01

Abstract

SIP networks use signalling monitoring tools to diagnose user reported problem and for regression testing if network or client software is upgraded. As networks grow and become interconnected, including connection via transit networks, it becomes impractical to predict the path that SIP signalling will take between clients, and therefore impractical to monitor SIP signalling end-to-end.

This draft describes requirements for adding an indicator to the SIP protocol which can be used to mark signalling as of interest to logging. Such marking will typically be applied as part of network testing controlled by the network operator and not used in regular client signalling. However, such marking can be carried end-to-end including the SIP terminals, even if a session originates and terminates in different networks.

Table of Contents

1. Introduction

If users experience problems with setting up sessions using SIP, their service provider needs to find out why by examining the SIP signalling. Also, if network or client software or hardware is upgraded regression testing is needed. Such diagnostics apply to a small proportion of network traffic and can apply end-to-end, even if signalling crosses several networks possibly belonging to several different network operators. It may not be possible to predict the path through those networks in advance, therefore a mechanism is needed to mark a session as being of interest to enable SIP entities along the signalling path to provide diagnostic logging. This draft describes the requirements for such a 'log me' marker for SIP signalling.

2. Requirements Language

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 RFC 2119 [RFC2119].

3. Motivating Scenario

Signalling for SIP session setup can cross several networks, and these networks may not have common ownership and also may be in differrent countries. If a single operator wishes to perform regression testing or fault diagnosis end-to-end, the separate ownership of networks that carry the signalling and the explosion in the number of possible signalling paths through SIP entities from the originating to the terminating user make it impractical to pre-configure logging of an end-to-end SIP signalling of a session of interest.

The figure below shows an example of a signalling path through multiple networks.

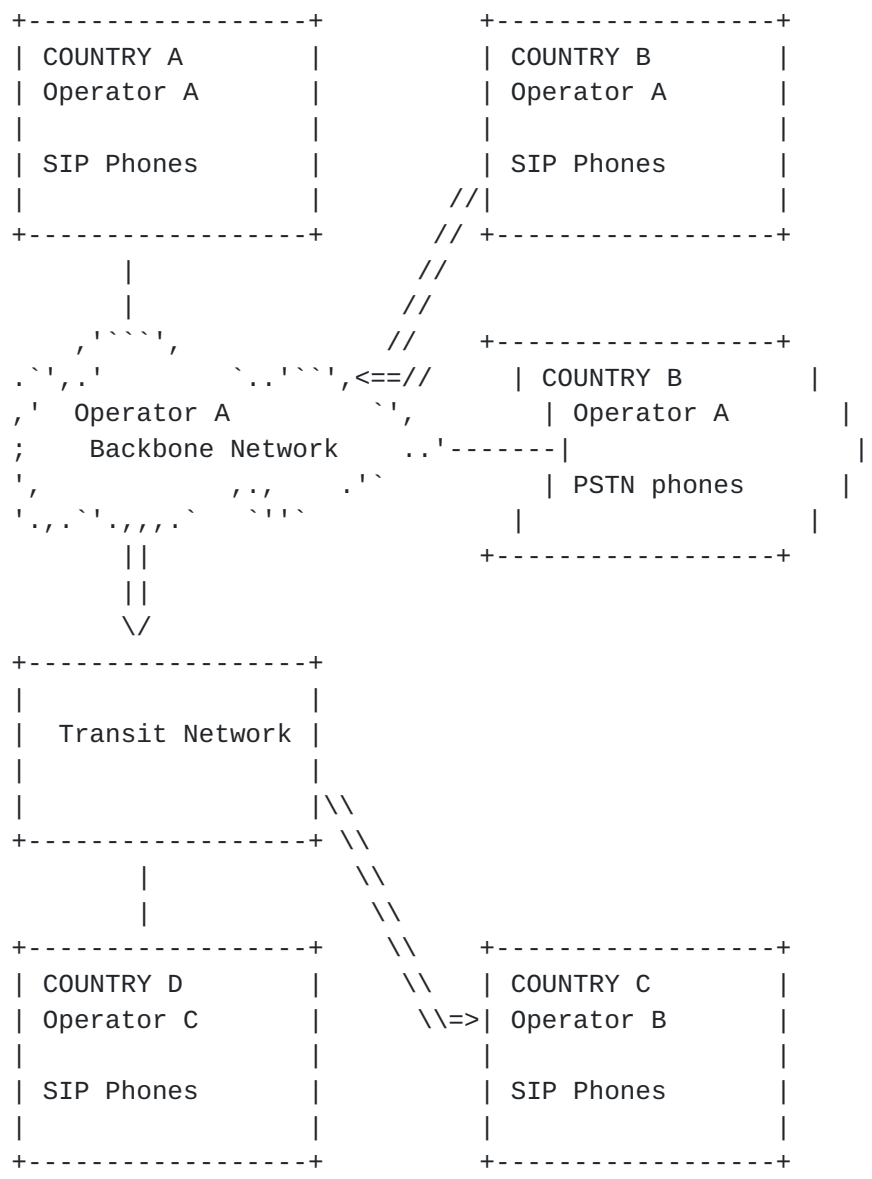

Figure 1: Example signalling path through multiple networks

4. Skeleton Diagnostic Procedure

The skeleton diagnostic procedure is as follows:

- The user's terminal is placed in debug mode. The terminal logs its own signalling and inserts a log me marker into SIP requests for session setup

- All SIP entities that the signalling traverses, from the first proxy the terminal connects to at the edge of the network to the destination client terminal, can detect that the log me marker is

present and can log SIP requests and responses that contain the marker if configured to do so.

- Subsequent responses and requests in the same dialog are logged.

- Logging stops, either because the dialog has ended or because a 'stop event', typically expiry of a certain amount of time, occurred

- The user's terminal and any other SIP entity that has logged signalling sends logs to a server that is co-ordinating diagnostics.

5. Requirements for a Log Me Marker

- REQ1: It shall be possible to mark a SIP request or response as of interest for logging by inserting a log me marker. This is known as log-me marking.

- REQ2: It shall be possible for a log-me marker to cross network boundaries.

- REQ3: A log-me marker is most effective if it passes end-to-end. However, source networks should behave responsibly and not leave it to a downstream network to detect and remove a marker that it will not use. A log-me marker should be removed at trust domain boundaries.

- REQ4: SIP entities should log SIP requests or responses with a log-me marker.

- REQ5: If a UA receives a request with a log-me marker, it shall echo that log-me marker in responses to that request.

- REQ6: A SIP proxy may perform log-me marking of requests and responses. Typical cases where a proxy needs to perform log-me marking are when a UA has not marked a request and when responses received on a dialog of interest for logging do not contain a log-me marker. In these cases, the entity that performs log-me marking is stateful inasmuch as it must remember when a dialog is of interest for logging.

- REQ7: For SIP proxies, logging of SIP requests that contain a log-me marker may be stateless. For example, it is not required for a SIP entity to maintain state of which SIP requests contained a log-me marker in order to log responses to those requests. Echoing a log-me marker in responses is the responsibility of the UA that receives a request.

- REQ8: A log-me marker may include an identifier that indicates the test case that caused it to be inserted, known as a test case identifier. The test case identifier does not have any impact on session setup, it is used by the diagnostic server to collate all logged SIP requests and responses to the initial SIP request in a dialog or standalone transaction. The Session-ID described in I-D.ietf-insipid-session-id-reqts [I-D.ietf-insipid-session-id-reqts] could be used as the test case identifier but it would be useful for the UA to log a human readable name together with this Session-ID when it performs log me marking of an initial SIP request.

6. Security Considerations

All drafts are required to have a security considerations section. See RFC 3552 [RFC3552] for a guide.

6.1. Trust Domain

Since a log me marker may cause a SIP entity to log the SIP header and body of a request or response, the log me marker should be removed at a trust domain boundary. If a prior agreement to log sessions exists with the net hop network then the log me marker might not be removed.

6.2. Security Threats

6.2.1. Log-me marking

The log me marker is not sensitive information, although it will sometimes be inserted because a particular device is experiencing problems.

The presence of a log me marker will cause some SIP entities to log signalling. Therefore, this marker must be removed at the earliest opportunity if it has been incorrectly inserted.

Activating a debug mode affects the operation of a terminal, therefore it must be supplied by an authorized server to an authorized terminal, it must not be altered in transit, and it must not be readable by an unauthorized third party.

Logged signalling is privacy-sensitive data, therefore it must be passed to an authorized server, it must not be altered in transit, and it must not be readable by an unauthorized third party.

6.2.2. Sending logged information

A SIP entity that has logged information should encrypt it, such that it can be decrypted only by the debug server, before sending it to a debug server in order to protect the content of logs from a third party.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

7.2. Informative References

[I-D.ietf-insipid-session-id-reqts] Jones, P., Salgueiro, G., Polk, J., Liess, L., and H. Kaplan, "Requirements for an End-to-End Session Identification in IP-Based Multimedia Communication Networks", draft-ietf-insipid-session-id-reqts-07 (work in progress), June 2013.

[RFC2234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3311] Rosenberg, J., "The Session Initiation Protocol (SIP) UPDATE Method", RFC 3311, October 2002.

[RFC3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C., and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC3903] Niemi, A., "Session Initiation Protocol (SIP) Extension for Event State Publication", RFC 3903, October 2004.

[RFC6086] Holmberg, C., Burger, E., and H. Kaplan, "Session Initiation Protocol (SIP) INFO Method and Package Framework", RFC 6086, January 2011.

Appendix A. Additional Stuff

This becomes an Appendix.

Author's Address

Peter Dawes
Vodafone Group
The Connection
Newbury, Berkshire RG14 2FN
UK

Email: peter.dawes@vodafone.com