Marking SIP messages to be logged

Keith Drage

On behalf of Peter Dawes

History

- Requirements generated by 3GPP and OMA.
- Various drafts:
  - draft-dawes-sipping-debug-id-01
  - draft-dawes-sipping-debug-event-01
  - draft-dawes-sipping-debug-05
- Presentation of drafts to INSIPID virtual interim in May 2012. Agreed that session-id could be basis for correlating logs, but needs separate signalling to initiate which is outside scope of INSIPID charter.
  - draft-kaithal-dispatch-sip-log-information-00
  - draft-dawes-dispatch-debug-00
  - draft-kaithal-dispatch-sip-log-information-00
- Discussion of draft-dawes-dispatch-logme-reqs-00 on DISPATCH list in December 2012.
- -01 draft of requirements draft published January 2013.

Scenario

- The skeleton diagnostic procedure is as follows (see section 4 of draft):
  - 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.

Requirements (1)

- draft-dawes-dispatch-logme-reqs-01 currently includes 9 requirements to be met by the solution. The purpose of this discussion is to agree on a charter description of the work, but the requirements are included here for information
  - 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.

Requirements (2)

- (continued)
  - 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.
  - REQ9: A log-me marker may include a locator of the server that collects logs. This locator is known as the diagnostic server identifier and may be an address of a server. A SIP entity can use the diagnostic server identifier to send collected logs to the diagnostic server.

Proposed charter text

- Proposal
  - 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 work will provide 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.
  - Milestones
    - Dec 2013 Requirements for marking SIP sessions for logging to IESG (Informational)
    - Mar 2014 Protocol for marking SIP sessions for logging to IESG (Proposed standard)
- note that the work does not necessarily need a new working group, it could for example be an extension of the work of either the SIPCORE WG or the INSIPID WG, but that is for the discussion to decide.