Internet-Draft

Intended status: Standards Track

Expires: December 30, 2009

Bell Laboratories, Alcatel-Lucent

H. Kaplan

AcmePacket

June 28, 2009

Reusing Transport Layer Connections in Session Initiation Protocol (SIP)
draft-jain-sip-transport-layer-connection-reuse-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the
provisions of BCP 78 and BCP 79. This document may contain material
from IETF Documents or IETF Contributions published or made publicly
available before November 10, 2008. The person(s) controlling the
copyright in some of this material may not have granted the IETF
Trust the right to allow modifications of such material outside the
IETF Standards Process. Without obtaining an adequate license from
the person(s) controlling the copyright in such materials, this
document may not be modified outside the IETF Standards Process, and
derivative works of it may not be created outside the IETF Standards
Process, except to format it for publication as an RFC or to
translate it into languages other than English.

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

This Internet-Draft will expire on December 30, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the
Abstract

The current Session Initiation Protocol (SIP) specification dictates that a transport layer connection can carry SIP requests in only one direction i.e. from the client to the server. This presents scalability problems as twice the number of connections are needed for each pair of SIP entities that communicate with each other. The internet-draft [I-D.ietf-sip-connect-reuse] specifies a mechanism for reusing SIP over TLS connections. However, that document is predicated on secure TLS mutual authentication and specifically refrains connection reuse for transports such as SIP over TCP and SCTP. There are many situations, such as in Trust Domains [RFC3324], where TLS mutual authentication may not be required but where connection reuse is beneficial. This document specifies connection reuse for SIP over connection-oriented transports such as TCP and SCTP. It specifies the same mechanism for connection reuse as specified in [I-D.ietf-sip-connect-reuse], however, the solution is presented in the context of Trust Domains.
# Table of Contents

1. Requirements notation ........................................... 4
2. Applicability Statement ....................................... 4
3. Introduction ..................................................... 4
4. Benefits of TCP, SCTP Connection Reuse ...................... 5
5. Overview of operation .......................................... 6
6. Requirements ..................................................... 6
7. Formal Syntax ................................................... 6
8. Normative Behavior .............................................. 6
9. Client Behavior .................................................. 6
10. Server Behavior ................................................ 8
11. Closing a TCP or SCTP connection ............................ 9
12. Security Considerations ....................................... 9
13. IANA Considerations ......................................... 10
14. References ..................................................... 10
14.1. Normative References ................................... 10
14.2. Informational References .................................. 10
Authors’ Addresses .................................................. 10
1. Requirements notation

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].

This document uses the concepts of Trust Domain and Spec(T), as specified in section 2.3 of RFC 3324 [RFC3324].

This document uses the same terminology as defined in section 1 of [I-D.ietf-sip-connect-reuse].

2. Applicability Statement

This document describes a mechanism that allows two SIP entities separated by a single hop that communicate over a connection-oriented transport protocol (e.g. TCP, SCTP) to reuse a connection for SIP requests sent in both directions. Many existing SIP implementations currently support this feature in their own proprietary ways. This document standardizes a mechanism for SIP over TCP and SCTP connection reuse.

This document makes use of the same SIP extension for connection reuse as the one specified in [I-D.ietf-sip-connect-reuse], except that the security considerations in this document are different. This document assumes that the SIP entities that make use of this mechanism are in a Trust Domain [RFC3324] or they have mutually authenticated themselves through some other means. Therefore, unlike [I-D.ietf-sip-connect-reuse], this document does not mandate TLS mutual authentication as a prerequisite for connection reuse.

3. Introduction

The current Session Initiation Protocol (SIP) [RFC3261] specification dictates that a transport layer connection can carry SIP requests in only one direction i.e. from the client to the server. This characteristic of SIP presents scalability problems as typically twice the number of connections are needed for each pair of SIP entities that communicate with each other.

The client and server roles in SIP are transactional. Therefore, there is no fundamental reason why SIP initiated connections cannot be reused for requests in both directions. An existing internet-draft [I-D.ietf-sip-connect-reuse] proposes a mechanism for reusing SIP over TLS connections. However, that specification is predicated on secure TLS mutual authentication and specifically refrains
connection reuse for transports such as SIP over TCP and SCTP.

There are many situations, such as in Trust Domains [RFC3324], where TLS mutual authentication is not required but where connection reuse is beneficial. This document enables connection reuse for SIP over TCP and SCTP transports. This document uses the same SIP extension for connection reuse as in [I-D.ietf-sip-connect-reuse] (the Via "alias" parameter), expect that the security considerations in this document are different.

This document assumes that the SIP entities that make use of the mechanism described here are in a Trust Domain [RFC3324] or they have mutually authenticated themselves through some other means. Therefore, unlike [I-D.ietf-sip-connect-reuse], this document does not mandate TLS mutual authentication as a prerequisite for connection reuse.

In the interest of avoiding duplication, this document only describes its differences from the SIP over TLS connection reuse document [I-D.ietf-sip-connect-reuse]. It frequently refers to the sections of [I-D.ietf-sip-connect-reuse] wherever there is commonality between the two documents.

Section 3 of [I-D.ietf-sip-connect-reuse] describes the unidirectional nature of connections for SIP requests in the current SIP specification and how their reuse is possible. That discussion also applies to SIP over TCP and SCTP transports and therefore this document.

4. Benefits of TCP, SCTP Connection Reuse

Section 4 of [I-D.ietf-sip-connect-reuse] describes the benefits of TLS connection reuse. Many of the benefits of TLS connection reuse also apply to TCP and SCTP connection reuse. Each new TCP connection requires a 3-way handshake. Each new SCTP association requires a 4-way handshake. These handshakes contribute to latency, post-dial delay, media clipping etc. Section 4 of [I-D.ietf-sip-connect-reuse] describes scenarios such as call flows involving frequent mid-dialog messages where connection reuse proves highly advantageous.

Connections consume resources on both hosts that terminate a connection. Connections require state management and periodic maintenance and therefore consume computing resources on both ends. This presents scalability and performance problems. Therefore, any technique that allows SIP entities to conserve and reuse connections is beneficial.
5. Overview of operation

Section 5 of [I-D.ietf-sip-connect-reuse] provides a tutorial on the operation of SIP over TLS connection reuse. Almost all of the discussion in that section including concepts such as the Via "alias" parameter, the columns in the alias table, the way RFC 3263 rules are applied are also applicable to SIP over TCP and SCTP connection reuse. The mention of TLS in the alias table and Via header example should be replaced with TCP or SCTP. In addition, any steps pertaining to X.509 certificate exchange should be ignored.

6. Requirements

Section 6 of [I-D.ietf-sip-connect-reuse] lists various requirements behind its proposed SIP over TLS connection reuse solution. All of those requirements apply to SIP over TCP and SCTP connection reuse as well. This document imposes an additional requirement:

1. The SIP entities that utilize the connection sharing mechanism MUST be members of a Trust Domain, T, and must comply to its Spec(T), as defined in section 2.3 of RFC 3324 [RFC3324].

7. Formal Syntax

Section 7 of [I-D.ietf-sip-connect-reuse] presents the formal syntax of the Via header "alias" parameter. The SIP over TCP and SCTP connection reuse mechanism uses the same parameter and the same formal definition.

8. Normative Behavior

This section is largely a duplication of section 8 of [I-D.ietf-sip-connect-reuse] except that all the normative text surrounding TLS and X.509 certificate exchange has not been carried over. Given that this section contains normative text, the authors felt that repetition of text from section 8 of [I-D.ietf-sip-connect-reuse] is necessary. The repetition is not verbatim, however. The text has been modified to reflect SIP over TCP and SCTP connection reuse.

9. Client Behavior

Clients SHOULD keep connections up as long as they are needed. Connection reuse works best when the client and the server maintain
their connections for long periods of time. Clients, therefore, SHOULD NOT automatically drop connections on completion of a transaction or termination of a dialog.

The proposed mechanism uses the Via header field parameter specified in [I-D.ietf-sip-connect-reuse]. The "alias" header field parameter is included in a Via header field value to indicate that the client wants to create a transport layer alias. The client places its advertised address in the Via header field value (in the "sent-by" production).

If the client places an "alias" header field parameter in the topmost Via header of the request, the client MUST keep the connection open for as long as the resources on the host operating system allow it to, and that the client MUST accept requests over this connection -- in addition to the default listening port -- from its downstream peer. And furthermore, the client SHOULD reuse the connection when subsequent requests in the same or different transactions are destined to the same resolved address.

Whether or not to allow an aliased connection ultimately depends on the recipient of the request; i.e., the client does not get any confirmation that its downstream peer created the alias, or indeed that it even supports this specification. Thus, clients MUST NOT assume that the acceptance of a request by a server automatically enables connection aliasing. Clients MUST continue receiving requests on their default port.

The client MUST also populate the destination IP address, port, and transport of the server in the alias table; these fields are retrieved from executing RFC3263 server resolution process on the next hop URI. And finally, the client MUST populate the alias descriptor field with the connection handle (or identifier) used to connect to the server.

Once the alias table has been updated with a resolved address, and the client wants to send a new request in the direction of the server, the client reuses the connection only if all of the following conditions hold:

1. The client uses the RFC3263 resolution on a URI and arrives at a resolved address contained in the alias table, and

2. The URI used for RFC3263 server resolution matches one of the identities stored in the alias table row corresponding to that resolved address.

Clients MUST be prepared for the case that the connection no longer
exists when they are ready to send a subsequent request over it. In such a case, a new connection MUST be opened to the resolved address and the alias table updated accordingly.

This behavior has an adverse side effect when a CANCEL request or an ACK request for a non-2xx response is sent downstream. Normally, these would be sent over the same connection that the INVITE request was sent over. However, if between the sending of the INVITE request and subsequent sending of the CANCEL request or ACK request to a non-2xx response, the connection was reclaimed, then the client SHOULD open a new connection to the resolved address and send the CANCEL request or ACK request there instead. The client MAY insert the newly opened connection into the alias table.

10. Server Behavior

Servers SHOULD keep connections up unless they need to reclaim resources. Connection reuse works best when the client and the server maintain their connections for long periods of time. Servers, therefore, SHOULD NOT automatically drop connections on completion of a transaction or termination of a dialog.

When a server receives a request over TCP and SCTP whose topmost Via header field contains an "alias" header field parameter, it signifies that the upstream client will leave the connection open beyond the transaction and dialog lifetime, and that subsequent transactions and dialogs that are destined to a resolved address that matches the identifiers in the advertised address in the topmost Via header field can reuse this connection.

Whether or not to use in the reverse direction a connection marked with the "alias" Via header field parameter ultimately depends on the policies of the server. It can choose to honor it, and thereby send subsequent requests over the aliased connection. If the server chooses not to honor an aliased connection, the server MUST allow the request to proceed as though the "alias" header field parameter was not present in the topmost Via header.

This assures interoperability with [RFC3261] server behavior. Clients can include the "alias" header field parameter without fear that the server will reject the SIP request because of its presence.

Servers MUST be prepared to deal with the case that the aliased connection no longer exists when they are ready to send a subsequent request over it. This can happen if the peer ran out of operating system resources and had to close the connection. In such a case, the server MUST open a new connection to the resolved address and the
alias table updated accordingly.

If the sent-by production of the Via header field contains a port, the server MUST use it as a destination port. Otherwise the default port is the destination port.

The server also populates the destination IP address, port and transport in the alias table from the topmost Via header field (using the ";received" parameter for the destination IP address). If the port number is omitted, a default port number of 5060 is to be used. And finally, the server populates the alias descriptor field with the connection handle (or identifier) used to accept the connection from the client (see Section 5 for the contents of the alias table.)

Once the alias table has been updated, and the server wants to send a request in the direction of the client, it reuses the connection only if all of the following conditions hold:

1. The server, which acts as a client for this transaction, uses the RFC3263 resolution process on a URI and arrives at a resolved address contained in the alias table, and

2. The URI used for RFC3263 server resolution matches one of the identities stored in the alias table row corresponding to that resolved address.

11. Closing a TCP or SCTP connection

Either the client of the server may terminate a TCP or SCTP connection. Before closing a TCP or SCTP connection, the initiator of the closure MUST either wait for any outstanding SIP transactions to complete, or explicitly abandon them.

After the initiator of the close has sent a closure alert, it MUST discard any TCP or SCTP messages until it has received a similar alert from its peer. The receiver of the closure alert MUST NOT start any new SIP transactions after the receipt of the closure alert.

12. Security Considerations

This specification assumes that the entities that make use of the SIP connection reuse mechanism described here are members of a Trust Domain, T, and they comply with its Spec(T), as defined in section 2.3 of RFC 3324 [RFC3324]. Connection reuse outside of a Trust Domain or between different Trust Domains is specified in SIP over
TLS connection reuse specification [I-D.ietf-sip-connect-reuse].

13. IANA Considerations

This document has no IANA actions.

14. References

14.1. Normative References

[I-D.ietf-sip-connect-reuse]
Gurbani, V., Mahy, R., and B. Tate, "Connection Reuse in the Session Initiation Protocol (SIP)",
draft-ietf-sip-connect-reuse-13 (work in progress),
March 2009.


14.2. Informational References


Authors’ Addresses

Rajnish Jain (editor)
IPC Systems
777 Commerce Drive
Fairfield, CT 06825
USA

Email: rajnish.jain@ipc.com
Vijay Gurbani  
Bell Laboratories, Alcatel-Lucent  
2000 Lucent Lane  
Rm 6G-440  
Naperville, IL 60566  
USA  
Email: vkg@lucent.com

Hadriel Kaplan  
AcmePacket  
Acme Packet  
71 Third Ave.  
Burlington, MA 01803  
USA  
Email: hkaplan@acmepacket.com