Scaling Requirements for Presence in SIP/SIMPLE
draft-ietf-sipping-presence-scaling-requirements-00.txt

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 on August 12, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

The document provides a set of requirements for enabling interdomain scaling in presence for SIP/SIMPLE. The requirements are based on a
separate scaling analysis document.

Table of Contents

1. Requirements notation ................................................. 3
2. Introduction .............................................................. 3
3. Suggested Requirements .................................................. 3
   3.1. Backward Compatibility Requirements .............................. 3
   3.2. Policy, Privacy, Permissions Requirements ....................... 3
   3.3. Scalability Requirements ............................................ 3
   3.4. Topology Requirements .............................................. 4
4. Conclusions ......................................................................... 4
5. Security Considerations .................................................... 5
6. Acknowledgments ............................................................. 5
7. References ......................................................................... 6
   7.1. Normative References .................................................. 6
   7.2. Informational References ............................................. 6
Authors’ Addresses ............................................................... 6
Intellectual Property and Copyright Statements ............................ 8
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 [1].

2. Introduction

The document lists requirements for optimizations of the SIP/SIMPLE protocol. These optimizations should reduce the traffic in interdomain presence subscriptions. The requirements are based on a separate scaling presence analysis document [4].

3. Suggested Requirements

In the presence scaling draft [4], several areas where the deployment of a presence system is far from being trivial are described, these include network load, memory load and CPU load. In this section lists an initial set of requirements for a solution that will optimize the interdomain presence traffic.

3.1. Backward Compatibility Requirements

- REQ-001: The solution should not hinder the ability of existing SIMPLE clients and/or servers from peering with a domain or client implementing the solution. No changes may be required of existing servers to interoperate.
- REQ-002: It does NOT constrain any existing RFC functional or security requirements for presence.
- REQ-003: Systems that are not using the new additions to the protocol should operate at the same level as they do today.

3.2. Policy, Privacy, Permissions Requirements

- REQ-004: The solution does not limit the ability for presentities to present different views of presence to different watchers.
- REQ-005: The solution does not restrict the ability of a presentity to obtain its list of watchers.
- REQ-006: The solution MUST NOT create any new or make worse any existing privacy holes.

3.3. Scalability Requirements

- REQ-007: It is highly desirable for any presence system (intra or inter-domain) to scale linearly as number of watchers and presentities increase linearly.
o REQ-008: The solution SHOULD NOT require significantly more state in order to implement the solution.

o REQ-009: It MUST be able to scale to tens of millions of concurrent users in each domain and in each peer domain.

o REQ-010: It MUST support a very high level of watcher/presentity intersections in various intersection models.

o REQ-011: Protocol changes MUST NOT prohibit optimizations in different deployment models esp. where there is a high level of cross subscriptions between the domains.

o REQ-012: New functionalities and extensions to the presence protocol SHOULD take into account scalability with respect to the number of messages, state size and management and processing load.

3.4. Topology Requirements

o REQ-013: The solution SHOULD allow for arbitrary federation topologies including direct peering and intermediary routing.

4. Conclusions

The document provides an initial list of requirements for a solution of scalability of interdomain presence systems using the SIP/SIMPLE protocol. The issue of scalability was shown in a separate document [4].

It is very possible that the issues that are described in this document are inherent to presence systems in general and not specific to the SIMPLE protocol. Organizations need to be prepared to invest a lot in network and hardware in order to create real big systems. However, it is apparent that not all the possible optimizations were done yet and further work is needed in the IETF in order to provide better scalability.

Nevertheless, we should remember that SIP was originally designed for end to end session creation and number and size of messages are of secondary importance for end to end session negotiation. For large scale and especially for very large scale presence the number of messages that are needed and the size of each message are of extreme importance. It seems that we need to think about the problem in a different way. We need to think about scalability as part of the protocol design. The IETF tends not to think about actual deployments when designing a protocol but in this case it seems that if we do not think about scalability with the protocol design it will be very hard to scale.

We should also consider whether using the same protocol between clients and servers and between servers is a good choice. It may be
that in interdomain or even between servers in the same domain (as between RLSs and presence servers) there is a need to have a different protocol that will be very optimized for the load and can assume some assumptions about the network (e.g. do not use unreliable protocol as UDP but only TCP).

When servers is connecting to another server using current protocol, there will be an extreme number of redundant messages due to the overhead of supporting UDP and to the need to send multiple presence documents for the same watched user due to privacy issue. A server to server protocol will have to address these issues. Some initial work to address these issues can be found in: [5], [6] and [7]

Another issue that is more concerning protocol design is whether NOTIFY messages should not be considered as media as audio, video and even text messaging. The SUBSCRIBE can be extended to do similar three way handshake as INVITE and negotiate where the notify messages should go, rate and other parameters. This way the load can be offloaded to a specialized NOTIFY "relays" thus not loading the control path of SIP. One of the possible ideas (Marc Willekens) is to use the SIP stack for the client/server NOTIFY but make use of a more optimized and controllable protocol for the server-to-server interface. Another possibility is to use the MSRP [2], [3] protocol for the notifies.

5. Security Considerations

This document discusses scalability requirements for the existing SIP/SIMPLE presence protocol and model. Many of the changes to the protocol will have security implications as mentioned in some of the requirements above.

One example of possible protocol changes that may have security implications is sending a presence document only once between domains in order to optimize the number of messages and network load. This possible optimization will delegate privacy protection from one domain to another domain and should be addressed when designing protocol optimizations.

Important part of work on the requirements and optimizations will be to make sure that all the security aspects are covered.

6. Acknowledgments

We would like to thank Jonathan Rosenberg, Ben Campbell, Markus Isomaki Piotr Boni, David Viamonte, Aki Niemi and Marc Willekens for
their ideas and input.

7. References

7.1. Normative References


7.2. Informational References


Authors’ Addresses

Avshalom Houri
IBM
Science Park Building 18/D
Rehovot,
Israel

Email: avshalom@il.ibm.com
Sriram Parameswar  
Microsoft Corporation  
One Microsoft Way  
Redmond, WA  98052  
USA  

Email: Sriram Parameswar@microsoft.com

Edwin Aoki  
AOL LLC  
360 W. Caribbean Drive  
Sunnyvale, CA  94089  
USA  

Email: aoki@aol.net

Vishal Singh  
Columbia University  
Department of Computer Science  
450 Computer Science Building  
New York, NY  10027  
US  

Email: vs2140@cs.columbia.edu  
URI:  http://www.cs.columbia.edu/~vs2140

Henning Schulzrinne  
Columbia University  
Department of Computer Science  
450 Computer Science Building  
New York, NY  10027  
US  

Phone: +1 212 939  7004  
Email: hgs+ecrit@cs.columbia.edu  
URI:  http://www.cs.columbia.edu/~hgs

Houri, et al.  
Expires August 12, 2008  
[Page 7]