Network Working Group
Request for Comments: 4092
Category: Standards Track

G. Camarillo
Ericsson
J. Rosenberg
Cisco Systems

June 2005

Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)

Status of This Memo

Copyright Notice

Abstract

This document describes how to use the Alternative Network Address Types (ANAT) semantics of the Session Description Protocol (SDP) grouping framework in SIP. In particular, we define the sdp-anat SIP option-tag. This SIP option-tag ensures that SDP session descriptions that use ANAT are only handled by SIP entities with ANAT support. To justify the need for such a SIP option-tag, we describe what could possibly happen if an ANAT-unaware SIP entity tried to handle media lines grouped with ANAT.

Table of Contents

1. Introduction

SIP [3] UAs (User Agents) often support different network address types. For example, a UA may have an IPv6 address and an IPv4 address. Such a UA will typically be willing to use any of its addresses to establish a media session with a remote UA. If the remote UA only supports IPv6, for instance, both UAs will use IPv6 to send and receive media.

The Alternative Network Address Types (ANAT) semantics [7] of the SDP [2] grouping framework [5] allow UAs to offer [4] alternative addresses of different types in an SDP session description. The IPv4/IPv6 dual-stack SIP UA of our previous example would generate an offer grouping an IPv6 media line and an IPv4 media line using ANAT. Upon receipt of this offer, the answerer [4] would accept one media line and reject the other.

If the recipient of an offer that uses ANAT supports the ANAT semantics, everything works as described in the ANAT specification [7]. Nevertheless, the recipient of such an offer (i.e., the answerer) may not support ANAT. In this case, different implementations of the answerer would react in different ways. This document discusses the answerer’s behaviors that are most likely to be found and describes their consequences. To avoid these consequences, we define the sdp-anat SIP option-tag.

The sdp-anat option-tag can be used to ensure that an offer using ANAT is not processed by answerers without support for ANAT. This option-tag can also be used to explicitly discover the capabilities of a UA (i.e., whether it supports ANAT).

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [1] and indicate requirement levels for compliant implementations.

3. The sdp-anat Option-Tag

We define the option-tag sdp-anat for use in the Require and Supported SIP [3] header fields. SIP user agents that place this option-tag in a Supported header field understand the ANAT semantics as defined in [7].

4. Backward Compatibility

Answerers without support for ANAT will react in different ways upon receipt of an offer using ANAT. We expect that, even under the same circumstances, different implementations will behave in different ways. In this section, we analyze these behaviors (i.e., the following subsections assume that the answerer does not support ANAT).

4.1. Answerer Supports All the Network Types Offered

If the answerer supports all the network types in the offer, it may accept the offer and establish all the media streams in it. This behavior is not what the offerer expects because it results in too many media streams being established. If the answerer starts sending media over all of them, the result may be a high bandwidth usage.

The answerer may also reject the offer, because although it supports all the network types in it, the answerer may not support them simultaneously. The error response sent by the answerer will most likely not be explicit enough about the situation. So, the offerer will not understand what went wrong.

In the previous scenarios, the sdp-anat option-tag would avoid the establishment of too many media streams and would allow the answerer to explicitly inform the offerer that the answerer did not support ANAT.

4.2. Answerer Does Not Support All the Network Types Offered

If the answerer does not support all the network types in the offer, it may only establish the media streams whose address types it understands and reject the rest. This would be an acceptable behavior from the offerer’s point of view.

On the other hand, the answerer may also reject the offer because it contains unknown address types. The error response sent by the answerer will most likely not be explicit enough about the situation. So, the offerer will not understand what went wrong.

In the previous scenario, the sdp-anat option-tag would allow the answerer to explicitly inform the offerer that the answerer did not support ANAT.

4.3. OPTIONS Requests

Although RFC 3388 [5] provides servers with a means to indicate support for ANAT in an SDP description, many servers do not include an SDP description in their responses to OPTIONS requests. The sdp-anat option-tag makes it possible to discover if any server supports ANAT, since they would include this option-tag in a Supported header field in their responses.

5. Option-Tag Usage

As discussed in the previous section, the use of the sdp-anat option-tag makes SIP messages more explicit about ANAT support. So, SIP entities generating an offer that uses the ANAT semantics SHOULD place the sdp-anat option-tag in a Require header field. SIP entities that support the ANAT semantics MUST understand the sdp-anat option-tag.

6. Security Considerations

An attacker may attempt to add the sdp-anat option tag to the Require header field of a message to perform a DoS attack. If the UAS does not support ANAT, it will return an error response instead of processing the message.

An attacker may attempt to remove the sdp-anat option-tag from the Require header field of a message. This may result in the establishment of too many media streams.

To avoid the previous attacks, integrity protection of the Require header field is RECOMMENDED. The natural choice to integrity protect header fields in SIP is S/MIME [6].

7. IANA Considerations

This document defines a SIP option-tag (sdp-anat) in Section 3. It has been registered by the IANA in the SIP parameter registry.

SIP user agents that place the sdp-anat option-tag in a Supported header field understand the ANAT semantics.

8. Normative References

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

[2] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[3] 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.

[4] Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)", RFC 3264, June 2002.

[5] Camarillo, G., Eriksson, G., Holler, J., and H. Schulzrinne, "Grouping of Media Lines in the Session Description Protocol (SDP)", RFC 3388, December 2002.

[6] Peterson, J., "S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)", RFC 3853, July 2004.

[7] Camarillo, G. and J. Rosenberg, "The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework", RFC 4091, June 2005.

Authors' Addresses

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

EMail: Gonzalo.Camarillo@ericsson.com

Jonathan Rosenberg
Cisco Systems
600 Lanidex Plaza
Parsippany, NJ 07054
US

EMail: jdrosen@cisco.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.