SIP FORUM

Carl Klatsky
Comcast
Gonzalo Salgueiro
Cisco
Olle E. Johansson
Edvina

Interoperability Impacts of IPv6 Interworking with Existing IPv4 SIP Implementations

SIP Forum Document Number: TWG-9

Abstract

This document captures potential impacts to IPv4 SIP implementations when interworking with IPv6 SIP implementations. Although some amount of interworking translation will occur at the network and application layers, an IPv4 SIP application may still encounter a SIP message with some IPv6 values in it, resulting in unforeseen error conditions. Such potential scenarios will be identified in this document so that SIP application developers can define solutions to handle these cases. Note, this document is not intended to be an exhaustive list, rather to provide an overview of some of the more commonly encountered potential scenarios.

Disclaimer

Carl Klatsky
Comcast
Gonzalo Salgueiro
Cisco
Olle E. Johansson
Edvina

Table of Contents

1. Introduction....3
2. Terminology and Conventions Used in This Document....3
3. Potential IPv4/IPv6 Interoperability Failure Scenarios....4
   3.1. IPv6 Address Handling in Via Headers....4
   3.2. IPv6 Address Handling in Record-Route and Route Headers....4
   3.3. IPv6 Address Handling in From / To / Contact Headers....4
   3.4. IPv6 Address Handling in SDP Body....4
   3.5. IPv6 Address Handling in 'reginfo' XML Registration Information Document....5
   3.6. IPv6 Address Handling in 30x Redirect....5
   3.7. IPv6 Address Handling in REFER-based Transfer....5
   3.8. DNS Resolution of IPv4/IPv6 in SRV Records....6
   3.9. IPv6 Address Handling in Multiple Contact Registrations....6
   3.10. Unsupported Address....6
4. Security Considerations....6
5. Appendix A: Additional Guidelines....7
   5.1. Appendix A.1: IPv6 Implementation Guidelines....7
   5.2. Appendix A.2: IPv6/IPv4 Interworking Function: Avoid IPv6 address Leakage?....7
References....9
6. Acknowledgements....11
7. Contributors....11
8. Full Copyright Statement....13

Carl Klatsky
Comcast
Gonzalo Salgueiro
Cisco
Olle E. Johansson
Edvina

1. Introduction

The continued proliferation of IPv6 infrastructure deployments has resulted in more IPv6 Session Initiation Protocol (SIP) User Agents (UAs) being turned up on the network. Considering the large deployed install base of IPv4 SIP UAs developed prior to the widespread deployment of IPv6, it is a well-known fact that not all IPv4 SIP UAs have taken into account all possible IPv4 SIP-to-IPv6 SIP interoperability considerations at the time of their development. The scenarios outlined in this document are intended as guidance for application developers to help identify solutions to resolve the identified interoperability challenges.

This document was inspired by tests at the SIPit interoperability events.

2. Terminology and Conventions Used in This Document

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].

[RFC 3261] defines additional terms used in this document that are specific to the SIP domain such as "proxy"; "registrar"; "redirect server"; "user agent server" or "UAS"; "user agent client" or "UAC"; "back-to-back user agent" or "B2BUA"; "dialog"; "transaction"; "server transaction".

This document uses the term "SIP Server" that is defined to include the following SIP entities: user agent server, registrar, redirect server, a SIP proxy in the role of user agent server, and a B2BUA in the role of a user agent server.

This document also uses the following terminology to make clear distinction between SIP entities supporting only IPv4, only IPv6 or supporting both IPv4 and IPv6.

- **IPv4-only UA/UAC/UAS:** An IPv4-only UA/UAC/UAS supports SIP signaling and media only on the IPv4 network. It does not understand IPv6 addresses.

- **IPv6-only UA/UAC/UAS:** An IPv6-only UA/UAC/UAS supports SIP signaling and media only on the IPv6 network. It does not understand IPv4 addresses.

- **IPv4/IPv6 UA/UAC/UAS:** A UA/UAC/UAS that supports SIP signaling and media on both IPv4 and IPv6 networks; such a UA/UAC/UAS is known (and will be referred to in this document) as a "dual-stack" [RFC4213] UA/UAC/UAS.

Carl Klatsky
Comcast
Gonzalo Salgueiro
Cisco
Olle E. Johansson
Edvina

3. Potential IPv4/IPv6 Interoperability Failure Scenarios

3.1. IPv6 Address Handling in Via Headers

As an IPv6 SIP message makes its way through the network, the Via header is updated and includes specific IPv6 addresses of IPv6 nodes that it has traversed. If the message arrives at an IPv4-only UAS it may still contain those IPv6 addresses in the Via header. Presumably the topmost Via header references an IPv4 address or a Fully Qualified Domain Name (FQDN) resolvable to any IPv4 address. In this case the IPv4-only UAS is able to send its response on to its next hop, otherwise the message would not have made it to the IPv4-only UA at all. The challenge for the IPv4-only UA then becomes to not generate an error even if the other Via headers that it does not need to act upon contain IPv6 addresses.

3.2. IPv6 Address Handling in Record-Route and Route Headers

Similar to the concerns of having IPv6 addresses in the Via headers, IPv4 SIP UAS may also encounter Record-Route headers that contain IPv6 addresses of IPv6 nodes the SIP message has traversed. It is again assumed that if the SIP message arrives at an IPv4-only UA that the topmost Record-Route header references an IPv4 address or a FQDN resolvable to any IPv4 address, such that the response may be routed back to a node reachable by the IPv4-only UAS. In this instance the IPv4-only UA should not generate an error when parsing the IPv6 addresses. Additionally, the IPv4-only UA may also need to populate the Route header in the response that includes the IPv6 addresses learned from previously received Record-Route header, and again do so without generating an error.

3.3. IPv6 Address Handling in From / To / Contact Headers

Another scenario with possible IPv6-to-IPv4 interoperability implications is the case where the IPv4-only UAS receives an IPv6 address in the Contact header and no Record-Route header. Since this represents the peer's reachable contact IP, it may not have been modified by any interworking element in the communications path. The IPv4-only UAS will have to send its requests through its outbound SIP server, and not generate an error upon receipt of a message with this IPv6 information.

In addition, using an IP address instead of domain in To and/or From headers may impact communication, as the From header is used for other communication sessions or added to a phone book.

3.4. IPv6 Address Handling in SDP Body

IPv4-only UASs may also receive SDP offers with IPv6 addresses in the Session Description Protocol (SDP) [RFC4566] portion of the message. An IPv6 address can appear in multiple places in the SDP, such as the o= line, c= line or a= lines (for Interactive Connectivity Establishment (ICE) [RFC5245]

attributes). A working assumption is that minimally the c= line will reference an IPv4 address of a media interworking element to allow the media communications being established by this session to work. Nonetheless the IPv4-only UAS needs be aware and properly handle any IPv6 addresses that may be within the received SDP.

3.5. IPv6 Address Handling in 'reginfo' XML Registration Information Document

There may be instances where an IPv4-only UAC subscribes to the registration event package [RFC3680] as a "watcher" for a specific entity, to be informed of registration state changes for that entity. The "watcher" may have no knowledge of the IP address family in use on the "watched" entity, and it is possible that a NOTIFY indicating an IPv6 address in the Extensible Markup Language (XML) [XML] body is received. The "watcher" needs to properly parse such a NOTIFY and provide the status update of the "watched" entity to the user or system that requested the information. This would be the case when an IPv6 SIP client registration is being "watched".

3.6. IPv6 Address Handling in 30x Redirect

There may be scenarios where an IPv4-only UAC receives a 30x redirect message in response to a request it has sent. This 30x message may contain a Contact header with an IPv6 address. This is the case where the call is being redirected to an IPv6-only UAS. Since this represents the peer's reachable contact IP, it may not have been modified by any interworking element in the communications path.

If the UAC has a configured outbound proxy the new call will be setup to that proxy. If that proxy is not dual stack, the call will fail. If there's no outbound proxy configured, the call will fail. If the UAC is a soft phone or hard phone, an error message should be displayed.

3.7. IPv6 Address Handling in REFER-based Transfer

After establishing a call between two IPv4-only UAs, one of the parties in the call may attempt to transfer the other party to a 3rd party using the REFER method [RFC5589]. This transfer may be to an IPv6-only UAS. The implication is that both IPv4-only UASs involved in the call transfer need to be able to handle a REFER with an IPv6 address in the Refer-To header. The transferor needs to be able to form the proper REFER message with the IPv6 Contact and the transferee needs to be able to process the REFER message and attempt to establish a call with the transfer target.

3.8. DNS Resolution of IPv4/IPv6 in SRV Records

A dual-stack UA may use the Domain Name System (DNS) SRV mechanism to resolve addresses of proxies that it needs to communicate with. In such a case it needs to be able to locate both IPv4 proxies and IPv6 proxies. This implies that the DNS server has been updated with both A and AAAA records for the SIP server, and that the dual-stack UA requests for both IPv4 and IPv6 SIP server addresses.

3.9. IPv6 Address Handling in Multiple Contact Registrations

A 200 OK to a REGISTER request might include multiple Contact headers because the user has registered his or her Address of Record (AOR) on multiple clients. Some of these Contact headers might have IPv6 addresses. An IPv4-only UAC must be able to handle the IPv6 information properly.

3.10. Unsupported Address

If the endpoint is an IPv4-only client and it receives a request with an SDP offer that has IPv6 address(es) only, the IPv4-only client should decline the request by returning 488 "Not Acceptable Here" (as defined in Section 13.3.1.2 of [RFC3261]) with Warning header that has warning code of 301 "Incompatible Network Address Formats" (as defined in Section 20.43 of [RFC3261]). If the IPv4-only client receives a request with an SDP offer that has a mixed set of IPv4 and IPv6 addresses, then the IPv4-only client should accept the IPv4 address(es) and decline the IPv6 address(es) by setting the port number in the m-line to zero.

4. Security Considerations

This document merely describes the potential impacts of IPv6 on IPv4 SIP implementations. The scenarios discussed in this informational document do not introduce any new security threats. The specific security vulnerabilities, attacks, threat models of the various protocols discussed in this document (SIP, SDP, ICE, etc.) are well documented in their respective documents.

Carl Klatsky
Comcast
Gonzalo Salgueiro
Cisco
Olle E. Johansson
Edvina

5. Appendix A: Additional Guidelines

Some additional interoperability guidelines are presented in this section.

5.1. Appendix A.1: IPv6 Implementation Guidelines

This section lists basic IPv6 recommendations for SIP implementations:

To avoid parsing errors, IPv6 address MUST be delimited by "[" and "]" in the following cases:

- If an IPv6 address is included in a SIP Request URI
- If an IPv6 address is included in a SIP "Via" header
- If an IPv6 address is included in a SIP "Contact" header

No delimiters are needed for other SIP tags such as "received" or even at the SDP level.

The SIP ABNF for IPv6 reference defined in [RFC3261] MUST NOT be used. Instead, rules defined in [RFC3986] MUST be supported.

To compare SIP URIs, [RFC5954] MUST be used instead of [RFC3261].

[RFC5952] MUST be supported for IPv6 textual representation purposes.

An IPv6-enabled SIP MUST NOT include any loopback address (::1) or link local address (fe80) in SIP headers and SDP body.

The offer/answer does not include IP Address in negotiation aspects and doesn't distinguish IPv4/IPv6. If the dual stack IPv4/IPv6 UAS receives an INVITE from IPv4 endpoint, based on Contact information, it should respond using the offer (IPv4/IPv6) in media/c= for better interoperability.

A IPv6 implementation parsers can be checked by running the test cases defined in [RFC5118].

5.2. Appendix A.2: IPv6/IPv4 Interworking Function: Avoid IPv6 address Leakage?

The introduction of IPv6-enabled SIP UAs may lead to some failure issues of the legacy (IPv4-only) UA are unable to parse IPv6 addresses. To prevent those failure cases, an IPv6/IPv4 Interworking Function may be deployed in the SIP infrastructure to adapt SIP messages. In particular, this interworking function may be configured to avoid leaking any IPv6 address to a legacy IPv4-only SIP UA (and vice versa). An IPv6-only SIP UA will be seen by a remote IPv4-only SIP UA as any legacy IPv4-only SIP UA. Leaking

IPv6 addresses in headers is a concern only for headers used for session routing purposes (e.g., topmost via, contact, etc.).

Within managed SIP networks, the impact of leaking addresses of distinct address family should be assessed through testing campaigns. If no failures are experienced, enabling the function which prevents leaking addresses of distinct address family may be avoided.

In order to promote the use of IPv6 transfer capabilities and avoid extensive usage of IPv4/IPv6 interworking resources, leaking IPv6 addresses in a backward compatible manner should be encouraged. For instance, the SDP offer can include both IPv4 and IPv6 addresses (e.g., [RFC6947]). The address family to be used to place the session will be decided by the remote peer.

When both IPv4 and IPv6 SIP UA are deployed in a network, the SIP Proxy Server will need a trigger to decide whether invoking IPv4/IPv6 Interworking function is required; otherwise IPv4/IPv6 IWF resources won't be optimized. A potential solution for this problem is discussed in [I-D.boucadair-dispatch-ipv6-atypes]. Relying on the address of contact is not deterministic since a dual-stack SIP UA may be registered with its IPv4 address while it supports also IPv6.

References

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

RFC 3261 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.

RFC 3680 Rosenberg, J., "A Session Initiation Protocol (SIP) Event Package for Registrations", RFC 3680, March 2004.

RFC3986 Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

RFC 4213 Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

RFC 4566 M. Handley, V. Jacobson, C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

RFC 5118 Gurbani, V., Boulton, C., and R. Sparks, "Session Initiation Protocol (SIP) Torture Test Messages for Internet Protocol Version 6 (IPv6)", RFC 5118, February 2008.

RFC 5245 Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

RFC 5589 R, Sparks, A. Johnston, D. Petrie, "Session Initiation Protocol Call Control – Transfer", RFC 5589, March 2009.

RFC 5952 Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.

RFC 5954 Gurbani, V., Ed., Carpenter, B., Ed., and B. Tate, Ed., "Essential Correction for IPv6 ABNF and URI Comparison in RFC 3261", RFC 5954, August 2010.

RFC6947 Boucadair, M., Kaplan, H., Gilman, R., and S. Veikkolainen, "The Session Description Protocol (SDP) Alternate Connectivity (ALTC) Attribute", RFC 6947, May 2013.

I-D.boucadair-dispatch-ipv6-atypes Boucadair, M., and Allen, A., "The atypes media feature tag for Session Initiation Protocol (SIP)", draft-boucadair-dispatch-ipv6-atypes-01 (work in progress), June 2013.

Carl Klatsky
Comcast
Gonzalo Salgueiro
Cisco
Olle E. Johansson
Edvina

XML Sperberg-McQueen, C., Yergeau, F., Bray, T., Maler, E., and J. Paoli, "Extensible Markup Language (XML) 1.0 (Fifth Edition)", World Wide Web Consortium Recommendation REC-xml-20081126, November 2008, <http://www.w3.org/TR/2008/REC-xml-20081126>.

6. Acknowledgements

The authors would like to acknowledge the support and contribution of the SIP Forum IPv6 Working Group. Mohamed Boucadair has contributed significant ideas and text. Dan Wing, Hadriel Kaplan, Paul Kyzivat, Dale Worley, and Neel Neelakantan have all provided a detailed review of the document and thoughtful comments.

7. Contributors

Carl Klatsky
Comcast
1717 Arch St.
Philadelphia, PA 19103
US

Email: carl_klatsky@cable.comcast.com

Olle E. Johansson
Edvina
Runbovaegen 10
Sollentuna SE-192 48
SE

Email: oej@edvina.net

Gonzalo Salgueiro
Cisco Systems
7200-12 Kit Creek Road
Research Triangle Park, NC 27709
US

Email: gsalguei@cisco.com

Andrew Hutton
Siemens Enterprise Communications
Technology Drive
Nottingham NG9 1LA
UK

Carl Klatsky
Comcast
Gonzalo Salgueiro
Cisco
Olle E. Johansson
Edvina

Email: andrew.hutton@siemens-enterprise.com

Rifaat Shekh-Yusef
Avaya
250 Sidney Street
Belleville, Ontario
Canada

Email: rifatyu@avaya.com

Carl Klatsky
Comcast
Gonzalo Salgueiro
Cisco
Olle E. Johansson
Edvina

8. Full Copyright Statement