Network Working Group
Internet-Draft
Updates: 5245, 6544 (if approved)
Intended status: Standards Track
Expires: January 17, 2013

A. Keranen
J. Arkko
Ericsson

July 16, 2012

Update on Candidate Address Selection for Interactive Connectivity Establishment (ICE) draft-keranen-mmusic-ice-address-selection-01

Abstract

This document revisits the rules on how candidate addresses are selected and combined when the Interactive Connectivity Establishment (ICE) NAT traversal method is used. This document updates RFCs 5245 and 6544.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on January 17, 2013.

Copyright Notice

Table of Contents

1. Introduction

When Interactive Connectivity Establishment (ICE) [RFC5245] [RFC6544] is used for NAT traversal, both endpoints gather multiple IP addresses and ports, also called candidate addresses, and test for connectivity between them. One of the principles of ICE is to gather all possible candidate addresses and pair them with all the addresses of the peer in order to test all combinations and get high probability for successful NAT traversal.

A prioritization formula is used by ICE so that most preferred address pairs are tested first, and if a sufficiently good pair is discovered, the tests can be stopped. Addresses obtained from local network interfaces, called host candidates, are recommended as high-priority ones to be tested first since if they work, they provide usually the best path between the two hosts. With IPv4 this approach works well since interfaces usually have just a single unicast IP address. However, with IPv6 addressing architecture [RFC4291] interfaces commonly have multiple addresses: global, link-local, Unique Local (ULA) [RFC4193], etc.

The ICE specification recommends to use the rules defined in [RFC3484] as part of the prioritization formula for IPv6 candidates, but does not give much further advice on how to handle different kind of IPv6 addresses. However, if all different kind of IPv6 addresses are paired with each other, some of the combinations will never work and may unnecessarily delay the completion of the ICE process.

This document updates the ICE rules defined in [RFC5245] and [RFC6544] on how candidate addresses are selected and how they should be combined with each other in order to maintain high performance for the ICE NAT traversal process.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

This document uses the same terminology as ICE (see Section 3 of [RFC5245]) and the following:

Local relayed candidate: a relayed candidate (obtained, e.g., from a TURN server) and included in an ICE offer or answer the agent has or will send.

3. Changes to Candidate Address Selection

This document proposes the following updates to the rules for selecting and combining IPv6 candidate addresses:

- Instead of RFC 3484 rules, the rules defined in [I-D.ietf-6man-rfc3484bis] MUST be used for determining the candidate priorities. If operating system address preferences are available (e.g,. via appropriate API extension), those SHOULD be used instead of default preferences.

- Deprecated IPv4-compatible IPv6 addresses [RFC4291] and IPv6 site-local unicast addresses [RFC3879] MUST NOT be included in the address candidates.

- Candidate addresses from link-local addresses MUST NOT be combined with any other candidates except other link-local candidates.

- Candidate addresses from Unique Local Addresses (ULAs) MUST NOT be combined with any other candidates except other ULA candidates.

- IPv4-mapped IPv6 addresses MUST NOT be included in the offered candidates unless the application using ICE does not support IPv4 (i.e., is an IPv6-only application [RFC4038]).

The following updates pertain to both IPv4 and IPv6 addresses:

- Addresses from a loopback interface MUST NOT be included in the candidate addresses.

- Local relayed candidates MUST NOT be combined with remote host candidates from IPv4 private address space [RFC1918] or IPv6 link-local addresses or ULAs.

4. Negotiating Address Selection Scheme

The prioritization method for the candidate address pairs used by ICE results in matching checklists for both endpoints and hence both endpoints start the checks for the same candidate pair roughly at the same time. This is important since in many scenarios a connectivity check initiated by both endpoints for the same pair is needed before a check for the pair succeeds. Also, some NAT devices have very short timeouts for their address translation bindings and a binding created by a connectivity check from one endpoint may expire before the corresponding connectivity check from the other endpoint is sent if there is a long delay between the two checks.

Depending on how different candidates are paired and whether RFC 3484 or the revised version of it [I-D.ietf-6man-rfc3484bis] is used, the endpoints may end up with different priorities and checklists. Therefore, the endpoints need to agree on how the address selection and pairing is done.

To indicate that the address selection and pairing rules defined in this document are used, the ICE offerer MUST include ice-options attribute with "bis-candidates" option identifier in the Session Description Protocol (SDP) [RFC4566] ICE offer. If the ICE offer does not include this option tag, the answerer SHOULD NOT utilize the updated rules defined in this document. If the offer included the option tag and the answerer supports this specification, the answerer SHOULD add the same option tag to the response and use the updated rules.

If the ICE answer does not contain the option tag, the offerer SHOULD NOT use the updated rules. However, even if the other endpoint does not indicate support for the updated rules, loopback addresses or the deprecated IPv6 addresses SHOULD NOT be included in the candidates.

5. Security Considerations

The general security considerations for ICE have been documented in Section 18 of [RFC5245] and Section 12 of [RFC6544]. The general security considerations for IPv6 address selection rules have been documented in [I-D.ietf-6man-rfc3484bis]. The vulnerabilities in ICE and RFC3484bis relate to attempts to hijack sessions opened through ICE, denial-of-service attacks, and accidental disclosure of private information. Mechanisms described in [RFC5245] and [RFC6544] - such as validated TCP connections - are designed to protect against connection hijacking.

Denial-of-service attacks can not be completely eliminated, but the amplification capabilities of ICE are limited through a maximum value of concurrently probed connections.

Any address probing mechanism opens up the possibility of outsiders learning the correlation between different IP addresses. For instance, the existence of a privacy address [RFC4941] in the candidate set along with other, more stable addresses will tell at least the peer and maybe eavesdroppers that the addresses are related.

This specification introduces no specific new security concerns beyond these, as it only attempts to unify the algorithms associated with candidate address pair selection. However, where address

selection rules in a node are configured through an external mechanism, as suggested in [I-D.ietf-6man-rfc3484bis], this opens up another avenue for introducing incorrect addresses into the probing mechanism. The resulting system is only as secure as its weakest component. For instance, even if sufficient security mechanisms are in place in ICE, vulnerabilities in the configuration mechanisms for the 3484bis priority tables may introduce weaknesses in the ability of ICE to select the right addresses.

6. IANA Considerations

IANA is requested to register "bis-candidates" option identifier under the "ICE Options" [RFC6336] registry. The required registration information is as follows:

Option identifier: bis-candidates

Contact: Ari Keranen, ari.keranen@ericsson.com

Change control: IETF

Description: Existence of this option identifier indicates that the revised rules (defined in RFCXXXX) are used for candidate address selection.

Reference: RFCXXXX

[RFC editor: replace XXXX with the RFC number of this document]

7. References

7.1. Normative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4566] Handley, M., Jacobson, V., and C. Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[RFC6336] Westerlund, M. and C. Perkins, "IANA Registry for Interactive Connectivity Establishment (ICE) Options", RFC 6336, July 2011.

[RFC6544] Rosenberg, J., Keranen, A., Lowekamp, B., and A. Roach, "TCP Candidates with Interactive Connectivity Establishment (ICE)", RFC 6544, March 2012.

[I-D.ietf-6man-rfc3484bis] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol version 6 (IPv6)", draft-ietf-6man-rfc3484bis-06 (work in progress), June 2012.

7.2. Informative References

[RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.

[RFC3879] Huitema, C. and B. Carpenter, "Deprecating Site Local Addresses", RFC 3879, September 2004.

[RFC4038] Shin, M-K., Hong, Y-G., Hagino, J., Savola, P., and E. Castro, "Application Aspects of IPv6 Transition", RFC 4038, March 2005.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

Appendix A. Acknowledgments

The authors would like to thank Jan Melen, Dan Wing, and Jonathan Lennox for comments, reviews and valuable input to the document.

Authors' Addresses

Ari Keranen
Ericsson
Jorvas 02420
Finland

Email: ari.keranen@ericsson.com

Jari Arkko
Ericsson
Jorvas 02420
Finland

Email: jari.arkko@piuha.net