

MMUSIC
Internet-Draft
Intended status: Standards Track
Expires: December 19, 2014

D. Wing
T. Reddy
P. Patil
P. Martinsen
Cisco
June 17, 2014

Mobility with ICE (MICE)
draft-wing-mmusic-ice-mobility-07

Abstract

This specification describes how endpoint mobility can be achieved using ICE.

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 December 19, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

MICE

June 2014

Table of Contents

1.	Introduction	3
2.	Notational Conventions	3
3.	Break Before Make	4
3.1.	Absence of other interfaces in Valid list	5
3.1.1.	Receiving ICE Mobility event	6
3.2.	Keeping unused relayed candidates active	7
3.3.	New STUN Attributes	8
4.	Make Before Break	8
5.	Comparison to ICE Restart and Trickle ICE	8
5.1.	Break Before Make - ICE Restart	9
5.2.	Break Before Make - Trickle ICE	10
6.	IANA Considerations	10
7.	Security Considerations	11
8.	Acknowledgements	11
9.	Change History	11
9.1.	Changes from draft-wing-mmusic-ice-mobility-00 to -01	11
9.2.	Changes from draft-wing-mmusic-ice-mobility-01 to -02	11
9.3.	Changes from draft-wing-mmusic-ice-mobility-02 to -03	11
9.4.	Changes from draft-wing-mmusic-ice-mobility-03 to -04	12
9.5.	Changes from draft-wing-mmusic-ice-mobility-04 to -05	12
9.6.	Changes from draft-wing-mmusic-ice-mobility-05 to -06	12
9.7.	Changes from draft-wing-mmusic-ice-mobility-06 to -07	12
10.	References	12
10.1.	Normative References	12
10.2.	Informative References	12
Appendix A.	13
A.1.	Presence of other interfaces in Valid list	13
A.1.1.	Receiving ICE Mobility event	14
A.2.	Losing an Interface	14
A.2.1.	Keeping unused candidates in the valid list active	15
	Authors' Addresses	16

Internet-Draft

MICE

June 2014

1. Introduction

When moving between networks, an endpoint has to change its IP address. This change breaks upper layer protocols such as TCP and RTP. Various techniques exist to prevent this breakage, all tied to making the endpoint's IP address static (e.g., Mobile IP, Proxy Mobile IP, LISP). Other techniques exist, which make the upper layer protocol ambivalent to IP address changes (e.g., SCTP). The mechanisms described in this document are in that last category.

ICE [[RFC5245](#)] ensures two endpoints have a working media path between them, and is typically used by Internet-connected interactive media systems (e.g., SIP endpoints). ICE does not expect either the local host or the remote host to change their IP addresses. Although ICE does allow an "ICE restart", this is done by sending a re-INVITE which goes over the SIP signaling path. The SIP signaling path is often slower than the media path (which needs to be recovered as quickly as possible), consumes an extra half round trip, and incurs an additional delay if the mobility event forces the endpoint to re-connect with its SIP proxy. When a device changes its IP address, it is necessary for it to re-establish connectivity with its SIP proxy, which can be performed in parallel with the steps described in this document. This document describes how mobility is performed entirely in the media path, without the additional delay of re-establishing SIP connectivity, issuing a new offer/answer, or the complications of multiple SIP offers. This document considers re-establishing bi-directional media the most critical aspect of a successful mobility event, and its efforts are towards meeting that goal.

This document proposes a mechanism to achieve RTP mobility when both endpoints support MICE. When both endpoints support MICE, ICE itself can be used to provide mobility. When only one endpoint supports MICE, a TURN server provides mobility as described in [[I-D.wing-tram-turn-mobility](#)]. Both mobility techniques work across and between network types (e.g., between 3G and wired Internet access), so long as the client can still access the remote ICE peer

or TURN server.

Readers are assumed to be familiar with ICE [[RFC5245](#)].

[2.](#) Notational Conventions

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 note uses terminology defined in [[RFC5245](#)], and the following

Wing, et al.

Expires December 19, 2014

[Page 3]

Internet-Draft

MICE

June 2014

additional terminology:

Break Before Make: The initially selected interface for communication may become unavailable (e.g due to loss of coverage when moving out of a WiFi hotspot) and new interfaces may become available due to administrative action (e.g manual activation of a specific connectivity technology) or due to dynamic conditions (e.g. Entering coverage area of a wireless network).

Make Before Break: The initially selected interface for communication may become deprioritized (e.g new interface becoming available and it's per bit cost is cheaper and the connection speed is faster than existing interface used for communication).

Simultaneous Mobility: If both the endpoints are mobile and roam at the same time between networks.

[3.](#) Break Before Make

When both endpoints support ICE, ICE itself can provide mobility functions. One of the primary aspects of ICE is its address gathering, wherein ICE has each endpoint determine all of the IP addresses and ports that might be usable for that endpoint and communicate that list of addresses and ports to its peer, usually over SDP. That enables the next primary aspect of ICE, which is its connectivity checks: each ICE endpoint sends a connectivity check from a checklist created by the local and remote candidates exchanged in the initial offer/answer exchange. When the ICE endpoint checks

the mapped address from the STUN response during ICE connectivity checks and finds that the transport address does not match any of the local candidates that the ICE agent knows about, the mapped address represents a new candidate -- a peer reflexive candidate. This will cause the endpoint to construct a new pair and insert it into the local checklist ([Section 7.2.1.3 of \[RFC5245\]](#)). ICE Mobility (MICE) takes advantage of that existing ICE functionality to provide faster mobility.

Endpoints that support ICE Mobility perform ICE normally, and MUST also include the MOBILITY-SUPPORT attribute in all of their STUN requests and their STUN responses. The inclusion of this attribute allows the ICE peer to determine if it can achieve mobility using ICE or needs to use TURN. To force the use of TURN to achieve ICE mobility, the ICE endpoint SHOULD NOT respond to ICE connectivity checks that have an IP address and port different from the TURN server, unless those connectivity checks contain the MOBILITY-SUPPORT attribute. In this way, the remote peer will think those other candidates are invalid (because its connectivity checks did not

succeed).

After concluding ICE and moving to the ICE completed state (see [Section 8 of \[RFC5245\]](#)) either endpoint or both endpoints can initiate ICE Mobility, no matter if it was the Controlling Agent or the Controlled Agent during normal ICE processing.

[3.1.](#) Absence of other interfaces in Valid list

When the interface currently being used for communication becomes unavailable then ICE agent acquires a list of interfaces that are available and based on the locally configured host policy preferences, the ICE endpoint performs ICE Mobility using one of the available interfaces. In this case local candidates from the selected interface are not present in the valid list. ICE Mobility is performed by:

1. The ICE agent remembers the remote host/server reflexive/peer reflexive candidates for each component of the media streams previously used from the valid list before clearing its ICE check list and ICE Valid List.

2. The ICE endpoint gathers host candidates of the same address family as the remote peer on the new interface, forms a check list by creating candidate pairs with local host candidates and remote host/server-reflexive candidates collected in step 1, performs "Computing Pair Priority and Ordering Pairs" ([Section 5.7.2 of \[RFC5245\]](#)), "Pruning the Pairs" ([Section 5.7.3 of \[RFC5245\]](#)), "Computing states" ([Section 5.7.4 of \[RFC5245\]](#)).
3. The ICE endpoint initiates ICE connectivity checks on those candidates from the check list in the previous step, and includes the MOBILITY-EVENT attribute in those connectivity checks.
4. The ICE endpoint acts as controlling agent and the ICE connectivity check from the previous step SHOULD also include the USE-CANDIDATE attribute to signal an aggressive nomination (see [Section 2.6 of \[RFC5245\]](#)).
5. The ICE endpoint performs "Discovering Peer Reflexive Candidates" ([Section 7.1.3.2.1 of \[RFC5245\]](#)), "Constructing a Valid Pair" ([Section 7.1.3.2.2 of \[RFC5245\]](#)), "Updating Pair States" ([Section 7.1.3.2.3 of \[RFC5245\]](#)), and "Updating the Nominated Flag" ([Section 7.1.3.2.4 of \[RFC5245\]](#)). When the valid list contains a candidate pair for each component then ICE processing is considered complete for the media stream and ICE agent can start sending media using the nominated candidate pair.

6. Once ICE connectivity checks for all of the media streams are completed, the controlling ICE endpoint follows the procedures in [Section 11.1 of \[RFC5245\]](#), specifically to send updated offer if the candidates in the m and c lines for the media stream (called the DEFAULT CANDIDATES) do not match ICE's SELECTED CANDIDATES (also see [Appendix B.9 of \[RFC5245\]](#)).

The ICE endpoint even after Mobility using ICE is successful can issue an updated offer indicating ICE restart if connectivity checks using higher priority candidate pairs are not successful.

Mobility using ICE could fail in case of Simultaneous Mobility or if the ICE peer is behind NAT that performs Address-Dependent Filtering (see [Section 5 of \[RFC5245\]](#)). Hence the ICE endpoint in parallel will re-establish connection with the SIP proxy. It will then

determine whether to initiate ICE restart under the following conditions:

- a. After re-establishing connection with the SIP proxy and before sending new offer to initiate ICE restart if Mobility using ICE is successful then stop sending the new offer.
- b. After successful negotiation of updated offer/answer to initiate ICE restart, proceed with ICE restart and stop Mobility using ICE if ICE checks are in the Running/Failed states or ICE is partially successful and not yet reached ICE complete state. It's not implementation friendly to have to two checks running in parallel. ICE restart can re-use partial successful ICE connectivity check results from Mobility using ICE if required as optimization.

3.1.1. Receiving ICE Mobility event

A STUN Binding Request containing the MOBILITY-EVENT attribute MAY be received by an ICE endpoint. The agent MUST use short-term credential to authenticate the STUN request containing the MOBILITY-EVENT attribute and perform a message integrity check. The ICE endpoint will generate STUN Binding Response containing the MOBILE-SUPPORT attribute and the ICE agent takes role of controlled agent. If STUN Request containing the MOBILITY-EVENT attribute is received before the endpoint is in the ICE Completed state, it should be silently discarded.

The agent remembers the highest-priority nominated pairs in the Valid list for each component of the media stream, called the previous selected pairs before removing all the selected candidate pairs from the Valid List . It continues sending media to that address until it finishes with the steps described below. Because those packets might

not be received due to the mobility event, it MAY cache a copy of those packets.

1. The ICE endpoint constructs a pair whose local candidate is equal to the transport address on which the STUN request was received with MOBILITY-EVENT, USE-CANDIDATE attributes and a remote candidate equal to the source transport address where the STUN request came from.

2. The ICE endpoint will add this pair to the valid list if not already present.
3. The agent sets the nominated flag for that pair in the valid pair to true. ICE processing is considered complete for a media stream if the valid list contains a selected candidate pair for each component and ICE agent can start sending media.

The ICE endpoint will follow Steps 1 to 3 when subsequent STUN Binding Requests are received with MOBILITY-EVENT and USE-CANDIDATE attributes.

3.2. Keeping unused relayed candidates active

The ICE endpoints can maintain the relayed candidates active even when not actively used, so that relayed candidates can be tried if ICE connectivity checks using other candidate types fails. The ICE agent will have to create permissions in the TURN server for the remote relayed candidate IP addresses and perform the following steps:

1. The ICE agent will keep the relayed candidates alive using Refresh transaction, as described in [[RFC5766](#)].
2. When the endpoint IP address changes due to mobility, the ICE agent will refresh it's allocation with TURN server using [[I-D.wing-tram-turn-mobility](#)].
3. The ICE agent will pair local and remote relayed candidates for connectivity checks when performing the steps in [Section 3.1](#).
4. If the ICE connectivity check succeeds only with local and remote relayed candidates, it suggests that either other peer is roaming at the same time or is behind Address-Dependent Filtering NAT. The ICE agent adds the relayed candidate pair to the valid list and marks it as selected. The ICE agent can now send media using the newly selected relayed candidate pair. The Mobile device must re-establish connection with SIP proxy, issue an updated offer indicating ICE restart so that media can switched to

This approach assists Mobility using ICE to succeed but brings in additional overhead of maintaining relayed candidates. In case of Simultaneous Mobility, host candidates can change for both the endpoints by maintaining relayed candidates and using [\[I-D.wing-tram-turn-mobility\]](#), media session can be established using the relayed candidate pair.

[3.3.](#) New STUN Attributes

Three new attributes are defined by this section: MOBILITY-EVENT, MOBILITY-SUPPORT.

The MOBILITY-EVENT attribute indicates the sender experienced a mobility event. This attribute has no value, thus the attribute length field MUST always be 0. Rules for sending and interpretation of receiving are described above.

The MOBILITY-SUPPORT attribute indicates the sender supports ICE Mobility, as defined in this document. This attribute has no value, thus the attribute length field MUST always be 0. Rules for sending and interpretation of receiving are described above.

[4.](#) Make Before Break

When a new interface comes up and initially selected interface becomes deprioritized (e.g. due to a low cost interface becoming available). The ICE endpoint re-connects to the SIP proxy using the new interface, gathers candidates, exchanges updated offer/exchange to restart ICE. Once ICE processing has reached the Completed state then the ICE endpoint can successfully switch the media over to the new interface. The interface initially used for communication can now be turned off without disrupting communications.

[5.](#) Comparison to ICE Restart and Trickle ICE

There has been some concern that ICE Mobility is unnecessary, and that an ICE restart ([section 9.1.1.1 of \[RFC5245\]](#)) would provide exactly the same functionality as ICE Mobility. These sections examine how ICE restart and Trickle ICE [\[I-D.rescorla-mmusic-ice-trickle\]](#) compare with ICE Mobility.

5.1. Break Before Make - ICE Restart

- o If ICE Restart is used for RTP Mobility then in case of Break before Make,
 1. Before the endpoint can send an ICE restart message, it has to first re-establish communication with its SIP proxy. This consumes one round-trip for both TCP and UDP. If the connection is protected with TLS (TCP) or DTLS (UDP), we can assume TLS session resumption [[RFC5077](#)] will be used to reduce the number of TLS messages. With TLS session resumption, this consumes 1 round trip. If TLS session resumption is not available, a full TLS handshake consumes 2 round trips. This is a total of 2 round trips (with session resumption) to 3 round trips (without session resumption), which is multiplied by the round trip time to the SIP proxy. The round trip time is dependent on a particular network or deployment, for example in second (2.5G), third (3G) generation wireless networks and satellite communication round trip time could be higher than 250ms. These calculations are only considering the network round-trip time and do not consider the wall-clock time to validate the TLS certificates or generate the TLS keys on the TLS client or the TLS server, which would make this longer.
 2. While performing the above steps to re-establish SIP connectivity with its SIP proxy, the endpoint will gather host candidates which incur no network traffic, server-reflexive candidates which incur a round-trip to a STUN server, and relayed candidates which incurs three round trips (two for re-authentication and one for creating the TURN permission). The STUN and TURN communications can be performed in parallel with the SIP connectivity check from step (1), above.
 3. The endpoints through the SIP server will exchange offer/answer. The SIP server could also be located halfway around the world from the endpoints and the delay could be significant. For SIP over UDP the endpoint will have send a SIP request and wait for the response to arrive.
 4. ICE restart requires sending a new INVITE. A new INVITE cannot be sent if there is an open SIP dialog, such as a previous INVITE. This means rapid mobility events will not work well, and there is also an increased likelihood for glare (both endpoints sending INVITES at the same time).

Internet-Draft

MICE

June 2014

[5.2.](#) Break Before Make - Trickle ICE

- o If Trickle ICE [[I-D.rescorla-mmusic-ice-trickle](#)] is used for RTP Mobility then in case of Break before Make,
 1. Trickle ICE can begin connectivity checks while the endpoint is still gathering candidates and can considerably shorten the time necessary for ICE processing to complete. It still involves the overhead of step 1 explained in section [Section 5.1](#).
 2. The endpoint would learn host candidates and inform them to the remote peer in offer, the remote peer will provide its candidates in answer. The host, server reflexive, peer reflexive and relayed candidates of the remote peer may not change and the remote peer does not have to gather the candidates again. Trickle ICE will test local host candidates with all types of remote candidates provided by the remote peer in the answer.
 - a. If the endpoint is not behind NAT and the ICE peer is behind NAT performing endpoint dependent filtering (or firewall blocking unsolicited incoming traffic) then ICE connectivity checks initiated by the endpoint to the remote peer will succeed as a consequence of suicide ICE connectivity check packets.
 - b. If the endpoint is behind NAT and ICE peer is behind endpoint-dependent filtering NAT then ICE connectivity checks using the first offer/answer will fail but will later succeed in subsequent offer/answer where the endpoint provides server-reflexive candidates.
 3. Trickle ICE must be supported by both endpoints for it be used.
- o If both endpoints support TRICKLE ICE then it is RECOMMENDED that TRICKLE ICE be tried instead of ICE restart in steps (a) and (b) of [Section 3.1](#).

[6.](#) IANA Considerations

IANA is requested to add the following attributes to the STUN attribute registry [[iana-stun](#)],

- o MOBILITY-EVENT (0x802, in the comprehension-required range)

Wing, et al.

Expires December 19, 2014

[Page 10]

Internet-Draft

MICE

June 2014

- o MOBILITY-SUPPORT (0x8000, in the comprehension-optional range)

[7.](#) Security Considerations

A mobility event only occurs after both ICE endpoints have exchanged their ICE information. Thus, both username fragments are already known to both endpoints. Each endpoint contributes at least 24 bits of randomness to the ice-ufrag ([Section 15.4 of \[RFC5245\]](#)), which provides 48 bits of randomness. An off-path attacker would have to guess those 48 bits to cause the endpoints to perform HMAC-SHA1 validation of the MESSAGE-INTEGRITY attribute.

An attacker on the path between the ICE endpoints will see both ice-ufrags, and can cause the endpoints to perform HMAC-SHA1 validation by sending messages from any IP address.

[8.](#) Acknowledgements

Thanks to Alfred Heggstad, Lishitao, Sujing Zhou, Martin Thomson, Emil Ivov for review and comments.

[9.](#) Change History

[Note to RFC Editor: Please remove this section prior to publication.]

[9.1.](#) Changes from [draft-wing-mmusic-ice-mobility-00](#) to -01

- o Updated [section 3](#)

[9.2.](#) Changes from [draft-wing-mmusic-ice-mobility-01](#) to -02

- o Updated Introduction, Notational Conventions, sections [3.1](#), [3.2](#).
- o Updated [section 3.5](#)

[9.3.](#) Changes from [draft-wing-mmusic-ice-mobility-02](#) to -03

- o Moved sections Presence of other interfaces in Valid list, Losing an Interface to Appendix.

Wing, et al.

Expires December 19, 2014

[Page 11]

Internet-Draft

MICE

June 2014

[9.4.](#) Changes from [draft-wing-mmusic-ice-mobility-03](#) to -04

- o Added [Section 6](#).

[9.5.](#) Changes from [draft-wing-mmusic-ice-mobility-04](#) to -05

- o Updated [Section 6](#).

[9.6.](#) Changes from [draft-wing-mmusic-ice-mobility-05](#) to -06

- o Updated [Section 5](#).
- o Added Implementation Status section.

[9.7.](#) Changes from [draft-wing-mmusic-ice-mobility-06](#) to -07

- o Removed Turn Mobility

[10.](#) References

[10.1.](#) Normative References

[I-D.wing-tram-turn-mobility]

Wing, D., Patil, P., Reddy, T., and P. Martinsen,

"Mobility with TURN", [draft-wing-tram-turn-mobility-00](#) (work in progress), June 2014.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", [RFC 5245](#), April 2010.
- [RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT (STUN)", [RFC 5389](#), October 2008.
- [RFC5766] Mahy, R., Matthews, P., and J. Rosenberg, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)", [RFC 5766](#), April 2010.

[10.2.](#) Informative References

- [I-D.rescorla-mmusic-ice-trickle]
Rescorla, E., Uberti, J., and E. Iovov, "Trickle ICE:

Wing, et al. Expires December 19, 2014 [Page 12]

Internet-Draft MICE June 2014

Incremental Provisioning of Candidates for the Interactive Connectivity Establishment (ICE) Protocol",
[draft-rescorla-mmusic-ice-trickle-01](#) (work in progress),
October 2012.

- [RFC5077] Salowey, J., Zhou, H., Eronen, P., and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", [RFC 5077](#), January 2008.
- [RFC5763] Fischl, J., Tschofenig, H., and E. Rescorla, "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)", [RFC 5763](#), May 2010.
- [RFC5780] MacDonald, D. and B. Lowekamp, "NAT Behavior Discovery Using Session Traversal Utilities for NAT (STUN)", [RFC 5780](#), May 2010.

- [RFC6263] Marjou, X. and A. Sollaud, "Application Mechanism for Keeping Alive the NAT Mappings Associated with RTP / RTP Control Protocol (RTCP) Flows", [RFC 6263](#), June 2011.
- [RFC6982] Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", [RFC 6982](#), July 2013.
- [iana-stun] IANA, "IANA: STUN Attributes", April 2011, <<http://www.iana.org/assignments/stun-parameters/stun-parameters.xml>>.

Appendix A.

[A.1.](#) Presence of other interfaces in Valid list

This technique is optional and only relevant if there is a host policy to maintain unused candidates on other interfaces using the steps in [Appendix A.2.1](#). ICE Agent can maintain unused candidates on other interfaces if it detects that it is behind Address-Dependent Filtering NAT or Firewall. ICE Agent can detect NAT, Firewall behaviour using the procedure explained in [\[RFC5780\]](#). When the interface currently being used for media communication becomes unavailable. If other interfaces are available and local candidates from these interfaces are already present in the valid list then ICE endpoint will perform the following steps:

Wing, et al. Expires December 19, 2014 [Page 13]

Internet-Draft MICE June 2014

1. The ICE endpoint based on the locally configured host policy preferences, will select a interface whose candidates are already present in the valid list.
2. The ICE endpoint clears all the pairs in the valid list containing the IP addresses from the interface that become unavailable.
3. The ICE endpoint initiates ICE connectivity checks on the selected interface. The ICE endpoint acts as controlling agent and MUST include MOBILITY-EVENT attribute to signal mobility

event and SHOULD also include the USE-CANDIDATE attribute to signal an aggressive nomination (see [Section 2.6 of \[RFC5245\]](#)). When all components have a nominated pair in the valid list, media can begin to flow using the highest priority nominated pair.

4. The ICE endpoint will re-establish connection with the SIP proxy. Once ICE connectivity checks for all of the media streams are completed, the controlling ICE endpoint follows the procedures in [Section 11.1 of \[RFC5245\]](#), specifically to send updated offer if the candidates in the m and c lines for the media stream (called the DEFAULT CANDIDATES) do not match ICE's SELECTED CANDIDATES (also see [Appendix B.9 of \[RFC5245\]](#)).

The ICE endpoint after Mobility using ICE is successful can issue an updated offer indicating ICE restart if higher priority interface becomes available.

[A.1.1.](#) Receiving ICE Mobility event

The ICE endpoint that receives ICE Mobility Event will perform the steps in [Section 3.1.1](#).

[A.2.](#) Losing an Interface

When an interface is lost, the SDP MAY be updated, so that the remote ICE host does not waste its efforts with connectivity checks to that address, as those checks will fail. Because it can be argued that this is merely an optimization, and that the interface loss might be temporary (and soon regained), and that ICE has reasonable accommodation for candidates where connectivity checks timeout, this specification does not strongly encourage updating the SDP to remove a lost interface.

Likewise, this specification recommends that ICE candidate addresses in valid list be maintained actively, subject to the host's policy. For example, battery operated hosts have a strong incentive to not

maintain NAT binding for server reflexive candidates learnt through STUN Binding Request, as the maintenance requires sending periodic STUN Binding Indication. As another example, a host that is receiving media over IPv6 may not want to persist with keeping a

NATted IPv4 mapping alive (because that consumes a NAT mapping that could be more useful to a host actively utilizing the mapping for real traffic).

Note: this differs from [Section 8.3 of \[RFC5245\]](#), which encourages abandoning unused candidates.

[A.2.1.](#) Keeping unused candidates in the valid list active

ICE endpoint subject to host policy can continue performing ICE connectivity checks using candidates from other interfaces on the host even after ICE is complete. If valid list contains unused candidate pairs from other interfaces and one of these interfaces can be selected to send to media in case the existing interface used for media is unavailable then ICE endpoint can keep the unused candidate pairs from other interface{s} alive by sending keepalives every NN seconds. It is recommended to only keep host/server-reflexive candidates active in the valid list and not the relayed candidates.

[A.2.1.1.](#) Sending keep alive requests

Application Mechanism for Keeping Alive the NAT Mappings Associated with RTP / RTP Control Protocol (RTCP) Flows [\[RFC6263\]](#) describes various reasons for doing keepalives on inactive streams and how to keep NAT mapping alive. However this specification requires some additional functionality associated with the keepalives.

STUN binding requests MUST be used as the keepalive message instead of the STUN Binding indication as specified in [\[RFC5245\]](#). This is to ensure positive peer consent from the remote side that the candidate pair is still active and in future mobility can be achieved using the steps in [Appendix A.1](#). The request must include the MOBILITY-SUPPORT attribute. If the STUN binding response matches a pair in the checklist then that candidate pair should be kept in the list. If the STUN transaction fails then the candidate pair will be removed from valid list.

[A.2.1.2.](#) Receiving keep alive requests

Upon receiving a STUN binding request containing a MOBILITY-SUPPORT attribute even when ICE processing is in the Completed state, the ICE endpoint will add this pair to the valid list if not already present and generate STUN Binding Response containing the MOBILE-SUPPORT attribute.

Authors' Addresses

Dan Wing
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134
USA

Email: dwing@cisco.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tiredy@cisco.com

Prashanth Patil
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marthalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: praspati@cisco.com

Paal-Erik Martinsen
Cisco Systems, Inc.
Philip Pedersens vei 22
Lysaker, Akershus 1325
Norway

Email: palmarti@cisco.com

