MMUSIC
Internet-Draft
Intended status: Standards Track
Expires: July 21, 2013

D. Wing
P. Patil
T. Reddy
P. Martinsen
Cisco

January 17, 2013

Mobility with ICE (MICE)
draft-wing-mmusic-ice-mobility-03

Abstract

This specification describes how endpoint mobility can be achieved using ICE. Two mechanisms are shown, one where both endpoints support ICE and another where only one endpoint supports 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 July 21, 2013.

Copyright Notice

Table of Contents

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.

A TURN [RFC5766] server relays media packets and is used for a variety of purposes, including overcoming NAT and firewall traversal issues and IP address privacy. The existing TURN specification does not allow the client address to change, especially if multiple clients share the same TURN username (e.g., the same credentials are used on multiple devices).

This document proposes two mechanisms to achieve RTP mobility: a mechanism where both endpoints support ICE, and a mechanism where only one endpoint supports ICE. When both endpoints support ICE, ICE itself can be used to provide mobility. When only one endpoint supports ICE, a TURN server provides 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 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 to that list of addresses and ports. A connectivity check may unknowingly traverse a NAT, which means the ICE endpoint receiving the connectivity check cannot validate the source IP address or port of the connectivity against the list of IP addresses and ports provided by the ICE peer. In fact, if the source IP address and port is not known to the ICE endpoint, it is added to the list of candidates (Section 7.2.1.3 of [RFC5245]. ICE Mobility takes advantage of that existent ICE functionality.

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 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 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]). An aggressive nomination allows sending media immediately after the connectivity check completes, without waiting for other connectivity checks to complete.

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 highest-priority 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 :

1. 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.

2. 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 Section 5.2.

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 higher-priority candidate pairs.

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 Section 5 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 indicate 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

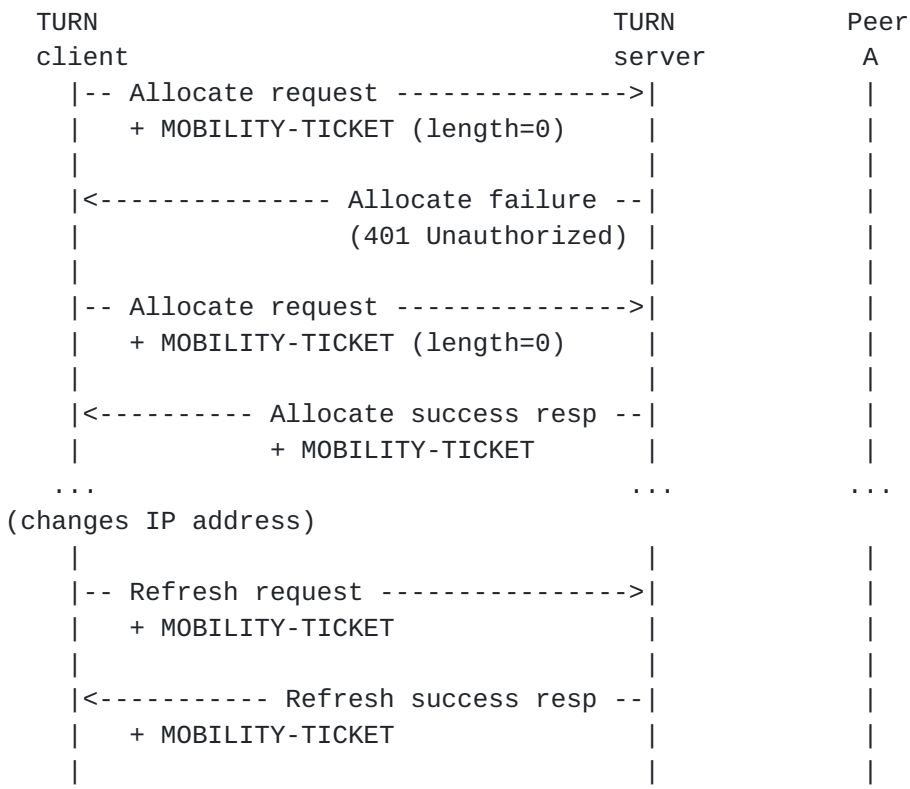
When a new interface comes up and initially selected interface becomes deprioritized (e.g due to a low cost interface becoming available). The ICE endpoint re-connects to the SIP proxy using the new interface, gather candidates, exchange updated offer/exchange to restart ICE. Once ICE processing has 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. Mobility using TURN

To achieve mobility, a TURN client should be able to retain an allocation on the TURN server across changes in the client IP address as a consequence of movement to other networks.

When the client sends the initial Allocate request to the TURN

server, it will also include the new STUN attribute MOBILITY-TICKET (with zero length value), which indicates that the client is capable of mobility and desires a ticket. The TURN server provisions a ticket that is sent inside the new STUN attribute MOBILITY-TICKET in the Allocate Success response to the client. The ticket will be used by the client when it wants to refresh the allocation but with a new client IP address and port. It also ensures that the allocation can only be refreshed this way by the same client. When a client's IP address changes due to mobility, it presents the previously obtained ticket in a Refresh Request to the TURN server. If the ticket is found to be valid, the TURN server will retain the same relayed address/port for the new IP address/port allowing the client to continue using previous channel bindings -- thus, the TURN client does not need to obtain new channel bindings. Any data from external peer will be delivered by the TURN server to this new IP address/port of the client. The TURN client will continue to send application data to its peers using the previously allocated channelBind Requests.



5.1. Creating an Allocation

5.1.1. Sending an Allocate Request

In addition to the process described in Section 6.1 of [RFC5766], the client includes the MOBILITY-TICKET attribute with length 0. This

indicates the client is a mobile node and wants a ticket.

5.1.2. Receiving an Allocate Request

In addition to the process described in Section 6.2 of [RFC5766], the server does the following:

If the MOBILITY-TICKET attribute is included, and has length zero, and the TURN session mobility is forbidden by local policy, the server MUST reject the request with the new Mobility Forbidden error code. Following the rules specified in [RFC5389], if the server does not understand the MOBILITY-TICKET attribute, it ignores the attribute.

If the server can successfully process the request create an allocation, the server replies with a success response that includes a STUN MOBILITY-TICKET attribute. TURN server stores it's session state, such as 5-tuple and NONCE, into a ticket that is encrypted by a key known only to the TURN server and sends the ticket in the STUN MOBILITY-TICKET attribute as part of Allocate success response.

The ticket is opaque to the client, so the structure is not subject to interoperability concerns, and implementations may diverge from this format. TURN Allocation state information is encrypted using 128-bit key for Advance Encryption Standard (AES) and 256-bit key for HMAC-SHA-256 for integrity protection.

5.1.3. Receiving an Allocate Success Response

In addition to the process described in Section 6.3 of [RFC5766], the client will store the MOBILITY-TICKET attribute, if present, from the response. This attribute will be presented by the client to the server during a subsequent Refresh request to aid mobility.

5.1.4. Receiving an Allocate Error Response

If the client receives an Allocate error response with error code TBD (Mobility Forbidden), the error is processed as follows:

o TBD (Mobility Forbidden): The request is valid, but the server is refusing to perform it, likely due to administrative restrictions. The client considers the current transaction as having failed. The client MAY notify the user or operator and SHOULD NOT retry the same request with this server until it believes the problem has been fixed.

All other error responses must be handled as described in [RFC5766].

5.2. Refreshing an Allocation

5.2.1. Sending a Refresh Request

If a client wants to refresh an existing allocation and update its time-to-expiry or delete an existing allocation, it will send a Refresh Request as described in Section 7.1 of [RFC5766]. If the client wants to retain the existing allocation in case of IP change, it will include the MOBILITY-TICKET attribute received in the Allocate Success response. If a Refresh transaction was previously made, the MOBILITY-TICKET attribute received in the Refresh Success response of the transaction must be used.

5.2.2. Receiving a Refresh Request

In addition to the process described in Section 7.2 of [RFC5766], the client does the following:

If the STUN MOBILITY-TICKET attribute is included in the Refresh Request then the server will not retrieve the 5-tuple from the packet to identify an associated allocation. Instead TURN server will decrypt the received ticket, verify the ticket's validity and retrieve the 5-tuple allocation from the contents of the ticket. If this 5-tuple obtained from the ticket does not identify an existing allocation then the server MUST reject the request with an error.

If the source IP address and port of the Refresh Request is different from the stored 5-tuple allocation, the TURN server proceeds with checks to see if NONCE in the Refresh request is the same as the one provided in the ticket. The TURN server also uses MESSAGE-INTEGRITY validation to identify the that it is the same user which had previously created the TURN allocation. If the above checks are not successful then server MUST reject the request with a 441 (Wrong Credentials) error.

If all of the above checks pass, the TURN server understands that the client has moved to a new network and acquired a new IP address. The source IP address of the request could either be the host transport address or server-reflexive transport address. The server then updates it's 5-tuple with the new client IP address and port. TURN server calculates the ticket with the new 5-tuple and sends the new ticket in the STUN MOBILITY-TICKET attribute as part of Refresh Success response.

5.2.3. Receiving a Refresh Response

In addition to the process described in Section 7.3 of [RFC5766], the client will store the MOBILITY-TICKET attribute, if present, from the

response. This attribute will be presented by the client to the server during a subsequent Refresh Request to aid mobility.

5.3. New STUN Attribute MOBILITY-TICKET

This attribute is used to retain an Allocation on the TURN server. It is exchanged between the client and server to aid mobility. The value is encrypted and identifies identifies session state such as 5-tuple and NONCE. The value of MOBILITY-TICKET is a variable-length value.

5.4. New STUN Error Response Code

This document defines the following new error response code:

Mobility Forbidden: Mobility request was valid but cannot be performed due to administrative or similar restrictions.

6. IANA Considerations

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

- MOBILITY-TICKET (0x802E, in the comprehension-optional range)
- MOBILITY-EVENT (0x802, in the comprehension-required range)
- MOBILITY-SUPPORT (0x8000, in the comprehension-optional range)

and to add a new STUN error code "Mobility Forbidden" with the value 501 to the STUN Error Codes registry [iana-stun].

7. Security Considerations

7.1. Considerations for ICE mechanism

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.

7.2. Considerations for TURN mechanism

TURN server MUST use strong encryption and integrity protection for the ticket to prevent an attacker from using a brute force mechanism to obtain the ticket's contents or refreshing allocations.

Security considerations described in [RFC5766] are also applicable to this mechanism.

8. Acknowledgements

Thanks to Alfred Heggestad, 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

- Updated section 3

9.2. Changes from draft-wing-mmusic-ice-mobility-01 to -02

- Updated Introduction, Notational Conventions, sections 3.1, 3.2.
- Updated section 3.5

9.3. Changes from draft-wing-mmusic-ice-mobility-02 to -03

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

10. References

10.1. Normative References

[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

[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.

[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 :

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

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

Email: praspati@cisco.com

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

Email: tireddy@cisco.com

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

Email: palmarti@cisco.com