Abstract

In the networks where multihomed hosts can have ULA and GUA addresses from different ISPs, multiple SIP signaling and media connectivity issues might arise due to inappropriate address selections. Some of the problems are described in [RFC5220]. Since SIP and SDP allow IP addresses to be embedded into their headers and lines, even if proper addresses are selected initially, SIP is not equipped with the mechanisms to respond to network events, and transition transport to reachable addresses. As a result, SIP messages and media might be filtered by routers, or discarded as unreachable destinations.

SIP protocol ([RFC 3261]) defines signaling messages and their headers. This document describes how a multihomed host should select addresses for SIP headers, like Contact and Via, to be reachable destinations. Host SHOULD change a default router for uplink failures, remove prefixes and addresses for unreachable ISP, and update contact address list.

SDP protocol ([RFC 3264]) defines how participants in a session select their parameters. This document describes how an offerer and answerer on multihomed hosts should select their addresses. If one of the selected addresses becomes unreachable, the document describes the mechanism how a new one should be selected and renegotiated.

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026 except that the right to produce derivative works is not granted.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.
Internet-Draft SIPv6 Address Selection on Multihomed Hosts January 2020

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt
The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

Copyright Notice

Copyright (c) 2019 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 (https://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.

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 [i].

Table of Contents

1. Introduction...................................................3
2. Terminology....................................................3
3. Problem Statement..............................................4
   3.1 Network Topology..........................................4
      3.1.1 Ingress filtered signaling source address & Non optimal data path 6
      3.1.2 Unreachable media destination address 7
      3.1.3 Ingress filtered media source address 7
      3.1.4 Unreachable listening media socket address 8
      3.1.5 Unreachable signaling ULA destination 8
      3.1.6 Unreachable media ULA destination 8
3.2 Background: Multi-Homed Hosts.............................8
3.3 Identified Problems.........................................9
3.4 Multihomed Host Unreachable due to Uplink Failure..........9
3.5 Multihomed Host INVITE Via Header Address Selection Issue.12
3.6 Multihomed Host SDP Address Selection Issues.............14
4. SIP Headers Address Selection...............................17
1. Introduction

It is common for enterprises to use two Internet Service Providers, ISPs, to access the Internet. When IPv6 is enabled, host in those networks have at least two IPv6 addresses, one for each ISP prefix. IPv6 only SIP clients on these hosts register one IPv6 address at which they can be reached. SIP Proxy forwards incoming INVITEs to the registered contact address. The address should be reachable. If SIP client registers all global IPv6 addresses, the list of addresses should be ordered and SIP Proxy should check the reachability, starting with the most preferred host IPv6 address.

When call sessions are initiated, the clients select one IPv6 address for Via header, the address to which 200 OK response will be delivered. When SIP Proxy forwards 200 OK to the offerers, the Via address should be reachable.

During media parameters negotiation, offerer and answerer set IPv6 address on which they listen to the media. Media streams should be able to reach these addresses.

2. Terminology

IPv6-only: an entity that uses only Internet Protocol version 6, IPv6, addresses

ISP: Internet Service Provider

SER: Site Edge Router. The router connecting a site to ISP uplink.

IPv6 Multihomed Host: Host with multiple IPv6 addresses

SASA: Source Address Selection (RFC 6724). Used by hosts to select the best source IPv6 address, given IPv6 destination address.

DASA: Destination Address Selection (RFC 6724). Used to select the best destination address, based on the available local addresses.

GUA: Global Unicast Address (RFC 3587). Enables hosts to be globally reachable.
ULA: Unique Local Address (RFC 4193). It is used for local communication and is not globally reachable.

SLAAC: Stateless Address Autoconfiguration (RFC 4862). An algorithm to auto-configure IPv6 addresses on hosts.

SDP: Session Description Protocol (RFC 3264 and RFC 6157)

RA: Router Advertisement (RFC 4861). A message multicasted from router to hosts. Used to assign IPv6 address prefixes to hosts for SLAAC usage and to announce its presence to hosts, after SER to ISP uplink recovery.

getsockname(): socket API function to get the socket SASA address from TCP or UDP socket.

connect(): socket API provides the remote IPv6 address to the socket SASA. (RFC 3493 & RFC 6316)

3. Problem Statement

A network topology, configuration and transient events can affect SIP signaling and media reachability. The transport protocols (like TCP or UDP) caring SIP signaling or RTP media might be unable to reach SIP hosts. Multihomed SIP hosts can experience:
- Unreachable signaling ULA destination,
- Unreachable signaling destination address,
- Ingress filtered signaling source address,
- Unreachable media ULA destination,
- Unreachable media destination address,
- Ingress filtered media source address,
- Unreachable listening media socket address, or
- Non optimal data path,
if a wrong IPv6 address is selected or, registered and negotiated addresses are not updated during network failures and recoveries.

3.1 Network Topology

The topology similar to https://tools.ietf.org/html/draft-ietf-rtgwg-enterprise-pa-multihoming-12#section-4.2 Figure 3, depicts multihomed SIP hosts Ha and Hb, SIP Proxy, and the IPv6 address assignment. The impact of uplink failure on Ha source address selection will be explained. Further analysis will show that algorithms for SIP and SDP address selection are needed to avoid reachability issues.

SITE-1 and SITE-2 have the same ISP-A and ISP-B service providers. ISPs assign their prefixes 2000::/64 and 3000::64. Ha, Hb, and SIP
Proxy have GUAs, created using ISP prefixes. R3 provides connectivity to an isolated local segment (aka a private LAN segment) and advertises ULA prefix. Ha and Hc have ULA addresses fc00::301 and fc00::401.

SERa and SERb first-hop routers are selected based on the source address prefixes [RFC8028]. The choice of Ha source address determines the selection of the first hop (SERa or SERb) router and ISP (ISP-A or ISP-B). If Ha selects 2000::201, packets would go over SERa to ISP-A. If SERa and SERb use ingress filtering, they would discard packets with source addresses that don’t have their prefixes (e.g. SERa would discard packets with 3000::/64 prefix). The figure below can be further simplified, with Ha directly connected to SERa and SERb, similar to SITE-2 topology.

When Ha needs to reach SIP Proxy at another site, it would use SASA to select the source address, using SIP Proxy preferred address (e.g. 2000::101) as a destination. All traffic to SIP Proxy would leave SITE-1 over the preferred ISP (e.g. ISP-A).
3.1.1 Ingress filtered signaling source address & Non optimal data path

In this scenario, SERa uplink to ISP-A fails on SITE-1. Ha uses SERa as the first hop router, when reaching SIP Proxy 2000::101, [RFC8028]. Ha source address is 2000::201, [RFC6724]. If uplink to ISP-A fails, and SERa does not redirect packets to SERb, the SIP signaling link breaks. To maintain the connectivity to SIP Proxy, Ha needs to use SERb as the first hop router, since SIP Proxy is reachable via SERb, and select 3000::301 source address to avoid ingress filtering on SERb. If Ha changes the default route to SERb (when SERa detects the uplink is down it sends RA with Router Lifetime of 0, indicating it
Internet-draft SIPv6 Address Selection on Multihomed Hosts January 2020

is no longer the default router) but selects ISP-A based 2000::201 source address (SERa sends RA with Valid Lifetime of 0, but some hosts don’t immediately remove the addresses with the expired prefix), and ingress filtering is enabled on SERb, SERb would discard the packets and send a Destination Unreachable message with Code 5 (Source address failed ingress/egress policy) back to Ha. Ha not only needs to change the default router to SERb, but also to expire 2000::201 and select 3000::301 when reaching SIP Proxy 2000::101.

In the same scenario, SIP Proxy is not aware that the uplink to ISP-A failed and attempts to send messages to the most preferred registered contact 2000::201, using its 2000::101 source address. ISP-A is unusable and would have to re-route packets over Internet to SERb, taking non-optimal route. Optimal route would be if SIP messages are sent over ISP-B, which would happen if SIP Proxy knows 2000::201 contact SHOULD NOT be used, and messages should be sent to the next preferred contact, 3000::301, destination over SERd. The contact list would be updated if, on the ISP-A uplink failure, Ha Re-REGISTERed with the new contact list (e.g with 3000::301).

In another scenario, SERc to ISP-A uplink fails on SITE-2. SIP Proxy does not know the uplink to ISP-A failed and would try to send messages to the most preferred registered contact 2000::201, using its 2000::101 source address, over SERc first hop router. The signaling link is broken. If SIP Proxy changes the default route to SERd (when it receives RA from SERc), but selects ISP-A based 2000::101 source address to reach 2000::201 contact, and ingress filtering is enabled, ISP-B would apply ingress filtering to source address prefix (e.g. 2000::/64) and SIP Proxy would not be able to talk to Ha.

3.1.2 Unreachable media destination address
If SERc uplink fails, the RTP media from Hb might be lost. Hb would not detect the uplink failure and would continue sending RTP packets to SERc, using previously offered Ha address (e.g. ‘c’=2000::201). SERc would not be able to deliver UDP media packets to Ha and would not notify Hb about the uplink failure.

3.1.3 Ingress filtered media source address
The ingress filtering might happen with Hb media, trying to reach Ha via ISP-B (SERc uplink failed) while using ISP-A based address (e.g. RTP SRC = 2000::102) for previously offered Ha address (e.g. ‘c’=2000::201). When the uplink fails, SERc can send RA with Router Lifetime of zero, and 2000::/64 prefix lifetime of zero. Hb can use this event to change the first hop router to SERd and expire its 2000::/64 address. If Hb still uses SDP negotiated Ha destination
3.1.4 Unreachable listening media socket address

Ha can open a listening socket using 2000::201 specific address and offer SDP ‘c’=3000::201. Hb media sent to 3000::201 would not be able to reach the listening socket.

3.1.5 Unreachable signaling ULA destination

Ha can select fc00::301 for registration or Via header, and SIP Proxy would not be able to send SIP INVITEs or 200 OK replies to ULA destination address.

3.1.6 Unreachable media ULA destination

Ha can select fc00::301 for SDP ‘c’ line and Hb would not be able to send media to ULA destination address.

3.2 Background: Multi-Homed Hosts

IPv6-only hosts can be assigned multiple IPv6 addresses, based on the prefixes from multiple ISPs. Socket, sending a packet, uses Source Address Selection, SASA, algorithm (RFC 6724), Rule 5.5, to select a source address for the prefix advertised by a default router. RFC 8028 extends the reachability range by selecting the source address based on the next hop router that can reach the destination. Based on RFC 8028, by selecting a source address a multi-homed host selects a first hop router to an ISP, using the source address prefix. draft-ietf-rtgwg-enterprise-pa-multihoming recommends mechanisms to detect an uplink to ISP failure and remove the prefix, default router, and host addresses for unreachable ISP. Unlike RFC 8028, where the source address selection was used to avoid BCP 38 source address filtering, several use cases will be analyzed to illustrate the problems when a wrong destination address is selected, or unreachable address is still used. Use cases illustrate
how ISPs ingress filtering, or site uplink failures, can cause signaling or media paths breakages.

3.3 Identified Problems

The Figure 2 below is used to illustrate SIPv6 signaling and media filtering or packet loss. Packets might not be delivered to GUA, Global Unicast Address, destination (a site uplink with ISP failed: draft-ietf-rtgwg-enterprise-pa-multihoming, or ingress filtering) or ULA destinations.

Multihomed HostA has at least two IPv6 addresses, each one based on ISP prefixes. A wrong address selection during SDP negotiation might cause RTP destination unreachability and ingress filtering.

3.4 Multihomed Host Unreachable due to Uplink Failure

In the Figure 2, When HostA registers to SIP Proxy in the same ISP1 domain (using RFC 3261), it selects IPv6 address for the Contact header. For incoming calls, SIP Proxy forwards the incoming INVITEs to the IPv6 contact address, provided during the registration. If HostA registers IPv6 address based on ISP1 prefix (e.g. 2000::/64 in Figure 1), SIP Proxy forwards INVITEs to HostA address (e.g. 2000::201). HostA can register a list of its preferred addresses, and SIP Proxy should use the list starting from the most preferred address.
Figure 2: SIPv6 INVITE to Failed Uplink

Figure 2 NOTE: HostA and SIP Proxy can be on different geographic locations serviced by the same ISP1 and ISP2. In case preferred message path from SIP Proxy to HostA is over ISP1, the destination address might not be routable, if uplink to ISP1 fails and SIP Proxy is still using HostA address with ISP1 prefix. Source address filtering might apply if SIP Proxy changes the default router but not the source address.
If HostA sends REGISTER over ISP1, using SASA selected ISP1 based contact (e.g. 2000::201 is selected as the best source address for SIP Proxy destination 2000::101), and the uplink R1-ISP1 fails after the registration, INVITE to HostA will be routed over R3-ISP1 and Internet to ISP1. The uplink R1-ISP1 failed and ISP1 would route INVITE over Internet to ISP2. The path is not optimal but INVITE would reach HostA over R2.

If uplink R3-ISP1 fails and SIP Proxy sends INVITE to R3, the INVITE will be lost.

If uplink R3-ISP1 fails and INVITE is to be sent to HostA, SIP Proxy might be able to use RA notification from R3 and change the default router to R4. If SIP Proxy still uses the old contact preference, it will select 2000::101 source address and R4 might apply ingress filtering to INVITE.
The solution for these problems is explained in section 4.1, REGISTER Contact Header Address Selection.

3.5 Multihomed Host INVITE Via Header Address Selection Issue

In some scenarios, R2 might provide connectivity to a private network. R2 might use ULA, Unique Local Address, address prefix 0xFD00::/7 (RFC 4193) for SLAAC, Stateless Address Autoconfiguration, assignments. Multihomed HostA would receive prefixes from both R1 and R2, and create at least one SLAAC GUA address based on ISP1 prefix, and at least one SLAAC ULA address, based on R2 prefix. When communicating with the external hosts, with GUA address, HostA should be able to select the ISP1 based global address. When talking to devices in the private network, it should select ULA address.
If HostA makes a call to HostB, it adds its IPv6 address to INVITE Via header (using RFC 3261). When HostB replies with 200 OK, SIP Proxy forwards the message to the topmost address in Via header (see RFC 3261). If HostA selects ULA address (e.g. fc00::301) for Via header, SIP Proxy forwards 200 OK to SER R3, and the 200 OK gets discarded since ULA destination address is not globally routable.
3.6 Multihomed Host SDP Address Selection Issues

SDP, Session Description Protocol, ([RFC 3264](https://tools.ietf.org/html/rfc3264) and [RFC 6157](https://tools.ietf.org/html/rfc6157)) Offerer IPv6 address might not be the best selected address on a multihomed host.

draft-gont-6man-address-usage-recommendation, section 3, recommends to bind() a listening socket to a specific address of a given scope, instead of to the unspecified address, to avoid attacks by narrowing the address scope. The offerer might open a listening media socket and selects the socket source address using the socket SASA to SIP Proxy destination (e.g. listen on 2000::201, instead of listening on any address). If the Offerer randomly select IPv6 address for SDP 'c' line (e.g. 3000::301 in Figure 1 or fc00::301 in Figure 2), a destination answerer might get a different IPv6 address in SDP 'c' line than the one selected by the offerer’s socket SASA, and the offerer might become unreachable.
Offerer’s socket would apply SASA for SIP Proxy address (e.g. 2000::101 would be passed to the socket connect() API) and select 2000::201 for the socket source address. SDP protocol does not have an algorithm for ‘c’ line address selection and might select unreachable address (e.g. fc00::301) for the ‘c’ line. If the answerer sends media to the offered address (e.g. fc00::301), media might not reach the Offerer, since fc00::301 is not globally routable.
In addition, if the offerer selects GUA SDP ‘c’ (e.g. 2000::201 on Figure 1), the media packets sent from the answerer (e.g. HostB), to HostA (e.g. 2000::201) address, might be filtered by ISP2. R3-ISP1 uplink fails, R3 sends RA to HB, telling the host R3 should not be used as default router. If HB does not expire 2000::/64 prefix and addresses, it might use SASA to select the source address for ‘c’=2000::201 destination, and select 2000::102 address. R4 would ingress filter the media with 2000::102 source address.
The solution to this problem is explained in detail in section 6, SDP Address Selection.

4. SIP Headers Address Selection

When a multi-homed host selects IPv6 address for a SIP header (e.g. Contact or Via header), it is important to select the address that will be reachable via the underlined network. SIP Signaling socket (e.g. TCP socket) solves the reachability problem by using the Source Address Selection, SASA, algorithm from RFC 6724, for a known destination.

For the examples exercised on Figure 1 and Figure 2:

- SIP REGISTER message is sent from HostA to SIP Proxy destination and the socket applies SASA to that destination, to select the packet source address, and
- SIP INVITE is sent from HostA to SIP Proxy destination and the socket applies SASA to that destination to select the packet source address.

The same socket SASA SHOULD be used to select the addresses for SIP headers, so SIP messages sent to the selected addresses will not be filtered out. getsockname() socket API can be used to obtain the SASA address for a known destination (passed in connect() socket API).

For the examples exercised on Figure 1 and Figure 2:

- SIP REGISTER message: HostA SHOULD use socket SASA to SIP Proxy destination and set the selected SASA address to REGISTER Contact header.

- SIP INVITE: HostA SHOULD use socket SASA to SIP Proxy destination and set the selected SASA address to INVITE Via header.

For the second and third problem in section 3.1.1, SERc SHOULD expire 2000::/64 prefix, so SIP Proxy SHOULD stop using 2000::101 address, change the default router to SERd, make 3000::301 the preferred Ha contact, and use 3000::101 as the source address, to talk to Ha 3000::301 over SERd.

The details about SASA improvements and dynamic address updates are in section 4.1.

4.1 REGISTER Contact Header Address Selection and Re-INVITE

Draft draft-ietf-rtgwg-enterprise-pa-multihoming recommends:

"A host is expected to be able respond dynamically to the failure of an uplink to a given ISP by no longer sending packets with the source address corresponding to that ISP."

The current SASA address selection does not solve this problem. The solution SHOULD update SASA rule 5.5 to check for the reachability and avoid using a prefix from the router over which destination is not reachable. That would make HostA select ISP2 based address (e.g. 3000::301) for the REGISTER contact, when the uplink to ISP1 fails and SIP Proxy address (based on ISP1 prefix) is the destination.

Another solution is provided by routers. When the reachability to a preferred ISP1 is lost, RA will be received from SERa for the unreachable ISP-A, with the preferred life time of zero, Router Lifetime of 0, and HostA SHOULD remove SERa as a default router, remove ISP1 based address (e.g. 2000::201) and send Re-REGISTER (to update contact to 3000::301) and Re-INVITE (to renegotiate 3000::301 IPv6 address) over SERb, using ISP-B based source address (e.g.
3000::301). Upon the uplink recovery, the contact and media addresses SHOULD be updated using SASA for the address selection. Next paragraph describes in details media address selection and renegotiation.

The first problem in the section 3.1.1 can be solved by SERa detecting the uplink failure and instructing R1 to expire ISP-A prefix. When RA message is received with the Router Lifetime of zero and 2000::/64 prefix lifetime of zero, Ha SHOULD change the default router to SERb, expire 2000::201 address, and use 3000::301 as the source address, while talking to SIP Proxy 2000::101 over SERb. Ha SHOULD Re-REGISTER the new contact 3000::301. SIP Proxy SHOULD immediately update its contacts and stop using 2000::201 destination.

SIP messages SHOULD be sent from SIP Proxy address selected for the HostA reachable destination. A solution might be for HostA to register a prioritized list of contact addresses, based on SASA and other policies. SIP Proxy SHOULD probe the contact addresses, starting from the most preferable one, till it finds a reachable one. SASA SHOULD be applied to the reachable destination address, and the selected SASA address would determine the first hop router. Hosts SHOULD be responsible to update the contact list based on network failures (a link to the first hop router or uplink to ISP failure) and recoveries.

5. SDP Address Selection

SDP ‘c’ line address selection needs to be defined for the initial offer from a multihomed host. Initially, the offerer does not have the answerer address. The selected IPv6 address might not be the best choice. A subsequent address selection might be needed to get the right offerer address.

SASA from RFC 6724 SHOULD be used to select the IPv6 address for SDP ‘c’ lines. If SASA is used it becomes apparent that:

- A destination address needs to be chosen for the initial offer. SASA SHOULD applied to that address and the result is used for ‘c’ line.

- When the offerer receives 200 OK and learns the destination address, the offerer might find the address selected during the initial SASA is not the right address.

To reach a destination (SDP answerer), SIP offer must go via SIP server. That is why SIP server IPv6 address SHOULD be used for the initial SASA.
When SDP negotiation is done, the offerer learns the answerer IPv6 address. The offerer applies SASA to the answerer preferred address. The initially offered IPv6 address might not be the best SASA address. This might cause the source IPv6 socket address in the subsequent media packets to be different than the initially offered SDP ‘c’ line address. To prevent this, the offerer SHOULD do the second SASA, using the answerer ‘c’ line address as the destination. If SASA returns a different source address, the offerer SHOULD send Re-INVITE to renegotiate media addresses and open a new socket, using the newly selected source address. The initial socket SHOULD be closed.

It is equally important for the answerer to apply SASA on the offered IPv6 address, when selecting the ‘c’ line address in 200 OK SDP.

If SDP offer has two IPs of different address families (ALTC in RFC 6947), an address selection algorithm is needed to select the address for the opposite address family. The second media line address SHOULD be selected using:

- SASA, if the SIP Proxy IP of the opposite address family is known.
- Otherwise, the algorithm for the best ‘guess’ for the second address SHOULD be applied:
  -- Select the IP of the opposite address family from the same interface from which the first IP was selected
  -- If the second address is IPv6, prefer an address with a bigger scope. Prefer global over ULA address.
  -- If the second address is IPv4, prefer a public over a private address.
  -- More rules can be added, like if there are multiple addresses of the same scope, prefer manual over DHCP over stateless addresses.

- Upon receiving of the offer, the answerer responds to the offer with the acceptance response (200 OK), using a preferred IP address from the offered SDP (e.g. a preferred ‘altc’ line) as a destination address for its SASA address selection. The selected address is set into preferred 200 OK SDP media line.

- The offerer now has the IP address of the destination host. If the source address, selected using the IP address from the acceptance response from the answerer, is the same IP address selected for the initial offer, the offerer address selection is completed.

- If the selected address in the previous step is different from the address in the initial offer, the offerer sends Re-INVITE, using the address selected in the previous step. The second media IP address, if needed, is selected using the rules above.
The side effect of Re-INVITE is that media path might be different, and more optimal, than the signaling path.

The offerer can advertise multiple IPv6 addresses in the initial SDP offer (ICE RFC 5245). The SASA preferred address, for SIP Proxy destination, SHOULD be the highest priority address. When the answerer sets SDP media address, or the host candidates, it SHOULD use Destination Address Selection, DASA, algorithm (RFC 6724) to select the preferred destination address for a media stream. The selected destination SHOULD be used during SASA to select the answerer preferred address. The answerer can offer the preferred address or the prioritized host candidate list.

6. Security Considerations

This document recommends the use of existing standards to address the SIP Signaling and Media address selection. The security recommendations in outlined standards should be followed.

7. IANA Considerations

There is no impact on existing SIP and IPv6 messages.

8. References

9. Acknowledgments

The author gratefully acknowledges the contributions of: Rifaat Shekh-Yusef.

Author’s Addresses

Dusan Mudric
Avaya
425 Legget Dr.
Ottawa, ON
K2K 3C9
Canada
Email: dmudric@avaya.com

Dragan Grebovich
Avaya
4655 Great America Parkway
Santa Clara, CA
95054
USA
Email: dgrebovich@avaya.com