6MAN Working Group
Internet-Draft
Updates: RFC5014, RFC6724 (if approved)
Intended status: Standards Track
Expires: April 23, 2021

D. Mudric
Ciena
A. Petrescu
CEA, LIST

October 20, 2020

Least-Common Scope Communications
draft-mudric-6man-lcs-01

Abstract

This draft formulates a security problem statement. The problem arises when a Host uses its Global Unicast Address (GUA) to communicate with another Host situated on the same link.

To address this problem, we suggest to select and use addresses of a least scope that are common.

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 https://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 April 23, 2021.

Copyright Notice

Table of Contents

1. Terminology

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 [RFC2119].

2. Problem Statement

Sockets listening on a global addresses are exposed to attacks. RFC6724 Rule 8 selects a candidate address with the smallest scope. Applications don't always have LL candidate address. They usually have a GUA address. If GUA is on a local link, an application will open a socket using GUA. To avoid using GUA on the local link, a sender needs to find a destination LL address. Currently SASA algorithm (RFC 6724 "Default Address Selection for Internet Protocol Version 6 (IPv6)") cannot use the smallest common scope, given destination GUA.

For security reasons, hosts should use an address with the smallest scope. To avoid these attacks, the host should use LL or ULA addresses.

These security reasons, in more detail, are described next. There is a security problem when a Host uses (one of) its Global Unicast Address(es) (GUA) to communicate to another Host situated on the same link. The problem appears even if that second Host uses its link-local address (LL) for this communication.

The problem is that the Host that uses the GUA to actively communicate with another Host situated on the same link opens a

globally reachable entry point in its operating system kernel. This entry point appears when the GUA is assigned to a socket structure. Were that address an LL, and not a GUA, that entry would not be globally reachable.

To realize communications between Hosts on the same link, it is sufficient to rather use LL addresses on both Hosts.

When a Host uses a GUA to communicate to another Host situated on the same link, it unnecessarily becomes an easy attack target. The attacker might be situated anywhere in the Internet (globally).

3. Least Common Scope Communications

It is recommended that a Host that needs to communicate with another Host that is situated in a particular scope, to use addresses of same scope, or of the least common scope.

For example, two Hosts situated on the same link should ideally use LL addresses to communicate to each other. An interpretation suggests that, given GUA and ULA, a least common 'scope' is the ULA scope (even though, formally, both ULA and GUA are of same global scope). But the global unicast addresses (GUAs) should not be used for two Hosts on the same link: the global scope is unnecessarily large; it unnecessarily opens doors to attacks.

4. LL Address Resolution

The operation of resolving an LL address (LL address resolution) is to find the link-local address that is assigned to the same interface as a GUA (or an ULA). This operation can be realized in several manners.

In one manner, the pair [GUA or ULA address; LL address] is stored in a distributed file such as the Active Directory or the DNS. The resolution operation is to query that file to find the LL address that corresponds to a GUA or ULA address. There are some issues to be considered. For example, typically the LL address is not assigned neither by DHCPv6 nor by RA (it is self formed by a Host when the interface is put up by using a universally known prefix "fe80::/10") then how would DNS get that LL address? Another example is: how to query DNS to request the LL address corresponding to an AAAA entry? (it is known how to query DNS to obtain the AAAA of an FQDN, but not the LL of an AAAA).

In another manner, the operation of resolving a link-local address (LL address resolution) is performed within the context of selecting

source and destination addresses within a Host. In that context, the following steps occur:

1. Given multiple destination addresses, the DASA selects GUA and ULA destination. The term 'DASA' designates the Destination Address Selection Algorithm.

2. The LL address resolution operation is performed for these GUA and ULA.

3. The GUA and the LL addresses are given as input to the SASA. The term 'SASA' stands for Source Address Selection Algorithm. The SASA selects LL.

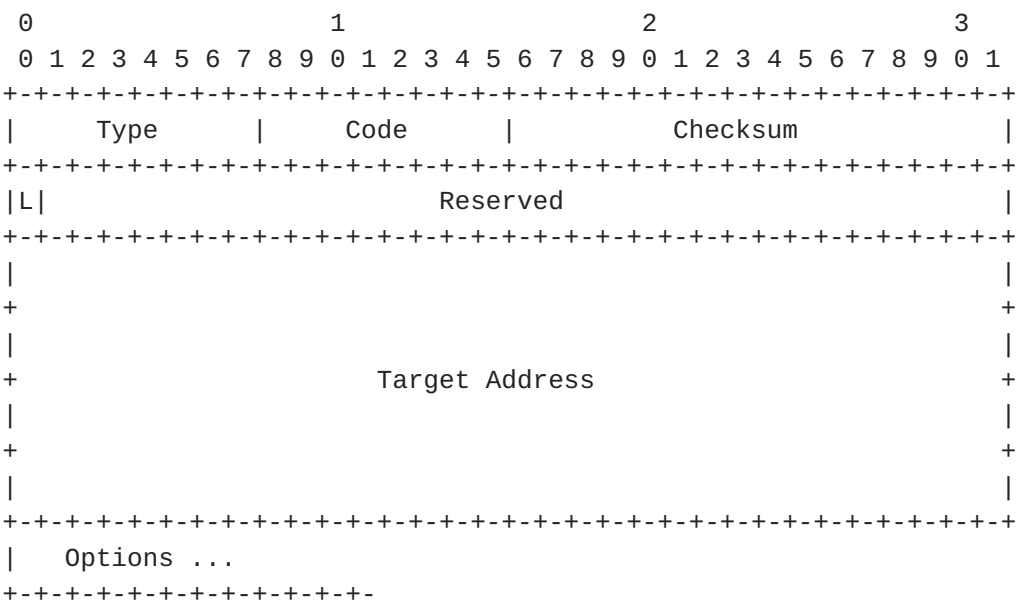
To facilitate LL communication on the local link, given a destination GUA or ULA:

- Prior to SASA, a host needs to check if a destination is ON-LINK
- for ON-LINK destination, a host needs to resolve the GUA or ULA destination address into a destination host LL address,
- a socket needs to open a port for the source LL address, and
- send packets to the destination LL address.

If both GUA and ULA destinations are known, and ULA destination is not on the link, SASA SHOULD use ULA address.

For the purposes of this document, Link Local (LL) address resolution is the process through which a host determines the Link Local address of a neighbor which is on the local subnet, given only neighbor's GUA or ULA IPv6 address (this 'address resolution' term is different than typical 'ND' term, or than the RFC4861 'address resolution' term which resolves an IP address into a MAC address). LL address resolution is performed only on addresses that are determined to be on-link and for which the sender does not know the corresponding Link Local address. Once the target LL address is learned, the communication sockets use LL addresses and are not exposed to security attacks.

For LL address resolution, 'L' flag is added to NS message. The Target-Address, TA, field in the NS message contains the address of the target of the solicitation (e.g., a host GUA or ULA address). The 'L' flag is added to Neighbor Solicitation Message, for LL address request



IP Fields:

Source Address
: If L bit is set, either LL address assigned to the interface from which this message is sent or (if Duplicate Address Detection is in progress [ADDRCONF rfc4861]) the unspecified address.

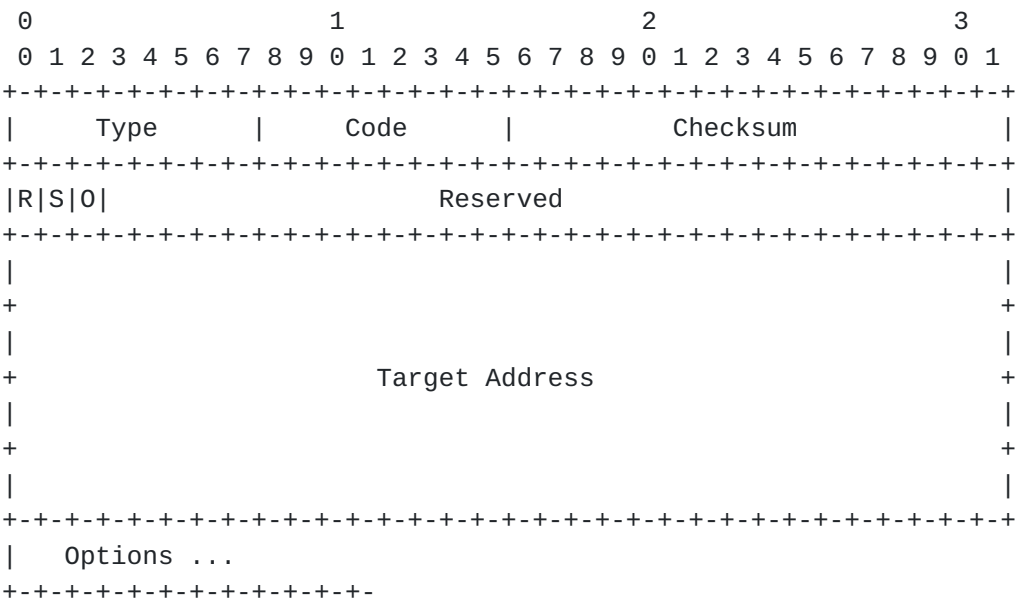
Destination Address
: Either the solicited-node multicast address corresponding to the target GUA or ULA address, or the target GUA or ULA address.

ICMP Fields:

L
: Link Local flag. When set, the L-bit indicates that the sender is requesting Link Local address from the target.

Figure 1: NS with 'L' bit

After receiving the Neighbor Solicitation message, the target returns its Link Local address in the Target Link-Local Address Option in a unicast Neighbor Advertisement, NA, message.



IP Fields:

Source Address
: If NS L bit is set, LL address of the same GUA target interface is provided

Possible options:

Target Link-Local address
: The Link Local address of the same GUA target, the sender of NA.

: This option MUST be included if NS L bit is set and LL is available.

Type 4 (Target Link Local address)

Length 16 bytes

Link Local Address: e.g. fe80:0:0:0:aa:bb:cc:dd

Receivers MUST silently ignore this option if they do not recognize it and continue processing the message.

Figure 2: NA for LL address resolution

The request for comments number 5014 [RFC5014], which treats about socket APIs, needs to be updated to use the given destination GUA or ULA addresses for ON-LINK determination, prior to SASA address selection; it also needs to be be updated to specify to send packets using LL address while talking to ON-LINK destinations.

5. Other Issues wih LL Address Resolution

If the Host 'switches' the destination address of an ongoing flow, between the GUA and the LL, there might interruptions in communications. The 'switching' behaviour depends on the application. Some applications (e.g. a particular application using the SIP protocol) the destination address is selected prior to opening the socket dedicated to streaming the media data. In such an application, a hard outage (e.g. interface down), might involve the creation of a new socket, and thus interruptions in media streaming. The question of maintaining an ongoing communication upon 'switching' between a GUA and an LL destination address is valid, for certain applications.

Multiple DNS aspects, for the resolution operation. Which LL address corresponds to a GUA?. How would DNS get that LL address?

6. Security Considerations

Security

7. IANA Considerations

IANA

8. Contributors

Contributors.

9. Acknowledgements

Mark Smith, Eduard Vasilenko.

10. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, DOI 10.17487/RFC5014, September 2007, <https://www.rfc-editor.org/info/rfc5014>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <https://www.rfc-editor.org/info/rfc6724>.

Appendix A. ChangeLog

The changes are listed in reverse chronological order, most recent changes appearing at the top of the list.

-00: initial version, with Dusan's comments.

Authors' Addresses

Dusan Mudric
Ciena

,

Canada

Phone:
+1-613-670-2425

Email:
dmudric@ciena.com

Alexandre Petrescu
CEA, LIST

CEA Saclay

Gif-sur-Yvette
,
Ile-de-France

91190

France

Phone:
+33169089223

Email:
Alexandre.Petrescu@cea.fr