draft-mudric-6man-lcs-00
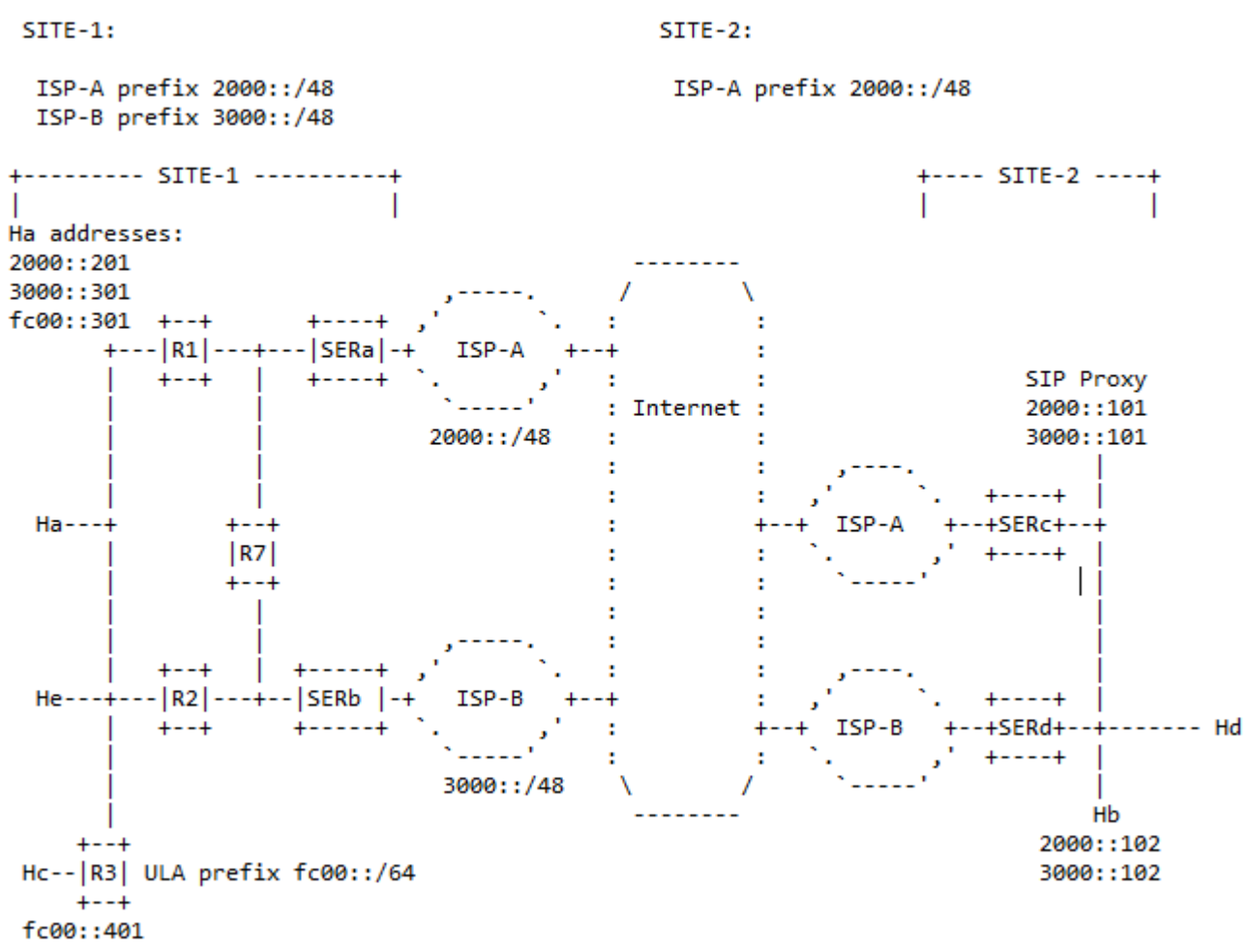
Least-Common Scope Communications

Dusan Mudric, Ciena
Alexandre Petrescu, CEA LIST

Problem Statement

```
SITE-1:                          SITE-2:

 ISP-A prefix 2000::/48           ISP-A prefix 2000::/48
 ISP-B prefix 3000::/48

     +--------- SITE-1 ----------+              +---- SITE-2 ----+
     |                           |              |                |
Ha addresses:
2000::201                              --------
3000::301                           ,-----.    /        \
fc00::301 +--+      +----+        ,'       `.  :          :
       +---|R1|---+--|SERa|-+   ISP-A   +--+  :          :
       |   +--+   |  +----+    `.       ,'  :          :      SIP Proxy
       |          |            `-----'    : Internet :      2000::101
       |          |                       :          :      3000::101
       |          |           2000::/48   :          :
       |          |                       :          :
       |          |                       :          :    ,-----.    +----+ |
  Ha---+          |                       +--+ ISP-A  +--+SERc+--+
       |       +--+                       :   `.    ,'  +----+ |
       |       |R7|                       :     `-----'        |
       |       +--+                       :                   | |
       |        |                         :
       |        |                         :
       |        |                         :
       | +--+   |  +-----+             ,-----.  :        ,----.    +----+ |
  He---+--|R2|---+--|SERb |-+   ISP-B   +--+  :      ,'     `.  +----+ |
       | +--+   |  +-----+    `.       ,'  :      :  ISP-B  +--+SERd+--+-------- Hd
       |        |            `-----'    +--+       `.    ,'  +----+ |
       |        |           3000::/48    \       /   `----'        |
       |        |                         --------                 Hb
     +--+                                                        2000::102
Hc--|R3| ULA prefix fc00::/64                                    3000::102
     +--+
fc00::401
```

- Hb-Hd: GUA for signaling and media sockets on SITE-2
- Sockets listening on global addresses are exposed to attacks

Problem Statement - cont

- RFC6724: DASA Rule 8 prefers a destination address with the smallest scope.

- Applications don't always have LL candidate address.

- An application will open a socket using GUA, even for GUA on a local link => exposed to attacks via globally reachable socket address
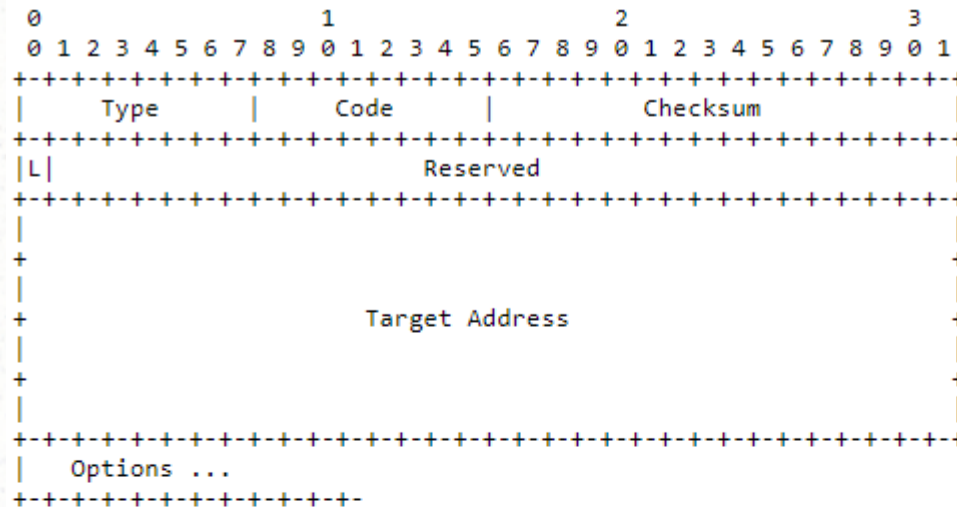
Proposed Solution (LL Address Resolution)

- To avoid these attacks use Link Local addresses for on-link communications

- Find a destination Link-Local address that is assigned to the same interface as an on-link GUA

Neighbor Solicitation 'L' bit

- For LL address resolution, 'L' flag is added to NS message

- NS Target-Address: is on-link GUA

- NS Source Address: if L bit is set, LL address

- NS Destination Address: GUA or Solicited Node Multicast Address

- NA: The target returns its LL address in the Target Link-Local Address Option

NS 'L' Bit Definition

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|L|                        Reserved                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                       Target Address                          +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Options ...
+-+-+-+-+-+-+-+-+-+-
```

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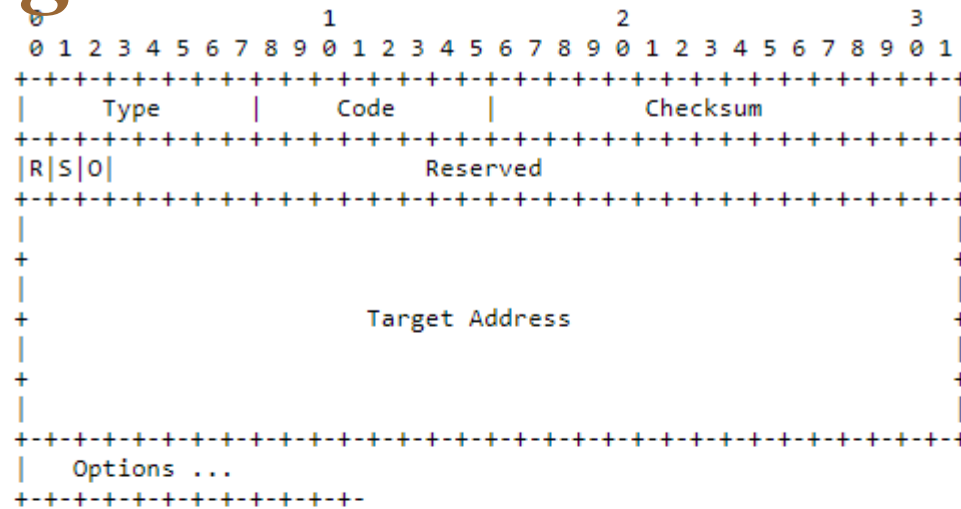   Either the solicited-node multicast address
            corresponding to the target GUA or ULA address, or the target
            GUA or ULA address.

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

NA Target Link-Local Address Option

```
                    0                   1                   2                   3
                    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |      Type     |      Code     |            Checksum           |
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |R|S|O|                         Reserved                        |
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |                                                               |
                   +                                                               +
                   |                                                               |
                   +                        Target Address                         +
                   |                                                               |
                   +                                                               +
                   |                                                               |
                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |   Options ...
                   +-+-+-+-+-+-+-+-+-+-

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
```

Questions?

- https://tools.ietf.org/html/draft-mudric-6man-lcs-00

- Thank you