

# Major Changes since savi-mix-03

- Text clean up to reflect the outcome of ieft79 to conform RFCs (FCFS used as the general rule)
- The main change is to describe a “tool” ( $\approx$  DAD-proxy) to allow the administrator to work-around FCFS and make bindings learn with one method preferred over (conflicting) bindings learnt with another.

# Scenarios and Introduction

- Current SAVI drafts review one particular address assignment/binding creation method:
  - SAVI-DHCP: stateful addresses assigned by DHCP
  - SAVI-FCFS: SLAAC addresses
  - SAVI-SEND: CGA addresses
- Real world is heterogeneous: not one but several assignment methods are used on the same link

# Problem Scope of SAVI-MIX

1. Define “conflicts”
2. Provide operational guidelines to avoid conflicts.
3. Provide a method to prevent them
4. Resolve conflicts when they occur.

Collisions happening within a given solution is outside the scope of this document.

# Define “conflicts”

- The binding table should be shared by all the solutions.
- Conflict  $\equiv$  collision
  - The same address is learnt from two different methods and bound to different anchors
- Review also the case when the anchors are the same

# Operational guidelines to avoid conflicts

Recommend that each solution has a dedicated address space.

- DHCP/Static: exclude the static address from DHCP pool.
- DHCP/SLAAC: separate prefix scope of DHCP and SLAAC.
  - Set the A bit in RA for SLAAC prefix. And set the M bit for DHCP prefix. [[RFC4861](#)] [[RFC4862](#)].
- SLAAC/Static: separate prefix scope of SLAAC and Static.
- SEND/non-SEND: impossible to avoid collisions – Deal withit

# Provide a method to prevent conflicts

- Enforce address space separation by enabling the switch to “defend” address spaces
- The switch sends DAD-NA (no LLA) upon address-space “violation”
- ADMIN driven:
  - Static binding
  - DHCP pool
  - Global vs Link-local
  - Etc .

# Resolve conflicts when they occur.

- 2.1 The same address is bound on **different binding anchors** by different SAVI solutions.
- 2.2 The same address is bound on the **same binding anchor** by different SAVI solutions.

# Referred RFCs for basic preference

- 1. “DAD MUST be performed on all unicast addresses prior to assigning them to an interface, **regardless of whether they are obtained through SLAAC, DHCPv6, or manual** configuration,...” [[RFC4862](#)]
- 2. **SLAAC**: "A tentative address that is determined to be a duplicate as described above MUST NOT be assigned to an interface,...” [[RFC4862](#)]
- 3. **DHCPv6** "The client SHOULD perform DAD on each of the addresses in any IAs it receives in the Reply message before using that address for traffic."  
[[RFC3315](#)]

# Referred RFCs for basic preference

- 4. **SeND**: A SEND node that uses the CGA authorization method to protect Neighbor Solicitations SHOULD perform DAD as follows. If DAD indicates that the tentative address is already in use, the node generates a new tentative CGA. If after three consecutive attempts no non-unique address is generated, it logs a system error and gives up attempting to generate an address for that interface. When DAD for the first tentative address, the node accepts both secured and unsecured NA and NS received in response to the NS. When performing DAD for the second or third tentative address, it ignores unsecured NA and NS." [[RFC3971](#)]
- 5. "The node MAY have a configuration option whereby it **ignores unsecured advertisements**, even when performing DAD for the first tentative address. This configuration option SHOULD be disabled by default. This is a recovery mechanism for cases in which attacks against the first address become common." [[RFC3971](#)]

# Conflict resolution

- 1. By default, SLAAC, DHCP and manually configured address by user have the **same** priority (FCFS).
- 2. SEND can have **higher** priority because it may configure an address bound by non-SEND node.

# Preference Table

<b>Candidate Existing</b>	<b>SLAAC</b>	<b>DHCP</b>	<b>SEND</b>	<b>Admin (for static or DHCP pool)</b>
<b>SLAAC</b>	scope of savi-fcfs	Prefer FCFS	Prefer SEND	Prefer Admin
<b>DHCP</b>	Prefer DHCP	scope of savi-dhcp	Prefer SEND	Prefer Admin
<b>SEND</b>	Prefer SEND	Prefer SEND	scope of savi-send	Prefer Admin
<b>Admin</b>	Prefer Admin	Prefer Admin	Prefer Admin	Prefer Candidate

# Multiple SAVI Device Scenario

- A single SAVI device doesn't have the information of all bound addresses on the perimeter. Therefore it is not enough to lookup local bindings to identify a collision.
- However, assuming DAD is performed throughout the security perimeter for all addresses regardless of the assignment method, then DAD response will inform all SAVI switches about any collision. In that case, FCFS will apply the same way as in a single switch scenario.
- If the admin configured on one the switches a range of addresses (or a single static binding) to defend, the DAD response generated by this switch will also prevent the binding to be installed on other switches of the perimeter.

## 2.2 Same address, Same Binding Anchor

- One binding entry may be set-up by different SAVI solutions in mixed scenario. No problem at binding setup.
- The problem: **collision in binding removal** is that one SAVI solution may require to remove a binding before binding lifetime of another SAVI solution expires
- Solution: keep a filtering entry in data plane as long as possible - remove only when it is required to be **removed by all SAVI solutions**

# Next Step

- Ask for adopting this document as a WG draft
  - Though the solutions still need enhancement, does this document provide a base for a WG future work ?

Thanks!