# MIF protocol drafts

## *draft-ietf-mif-mpvd-dhcp-support-02*
## *draft-ietf-mif-mpvd-ndp-support-02*
## *draft-ietf-mif-mpvd-id-01*

*Suresh Krishnan, Jouni Korhonen,*
*Shwetha Bhandari, Sri Gundavelli*

# Status

- Drafts completed working group
- Received low volume of reviews
- Reviews from Ian Farrer, Steven Barth, Tommy Pauly and Lorenzo Colitti (Thanks!!)

# Signature

- Do we want to keep the authentication parts of the container options?
  - Section 3.2 of RFC7556 requires authentication for the source and the integrity of the message
    - Do we still want this?
- Comments mentioned that they are complicated and not very useful
  - They also break some deployment models (e.g. homenet) as a side effect

# Editorial and clarity issues

- There are some issues raised with unclear wording in the drafts
- These will be put into an issue tracker and resolved
  - If some issues require substantive changes will gate on WG input

# DHCPv6

# Allowable options

- Which of the DHCPv6 options are allowable inside the container
  - All possible DHCPv6 options
    - Future proof but vague and error prone
  - Make an allowed list
    - Issues with future expansion
  - Make a IANA registry with a list of allowed options
    - Overhead of checking

# Replay protection

- The authentication options as defined today lack any built-in replay protection
- Do we need replay protection?
  - What *actually* breaks?
- This can be built in but it would require frequent updates from the originator of the configuration to the entity sending out the configuration information
- What does the WG think is the right compromise?

# Nesting

- Is nesting allowed or not?
  - i.e. PVD inside PVD
- We recommend not having it
  - Anyone against?

# Neighbor Discovery

# Space efficiency

- Authentication information can make the RAs very large
- Potential duplication of information inside PVDs exacerbates this further
- Should we limit contents of containers to a core set of options?

# Usage of info inside container

- Should the mif drafts specify how hosts handle information received inside containers?
  - Given that other configuration information definitions don't do this, should we?

# Security

- Hosts have no mechanism to specify that they do not want authenticated containers
- What do we want to do?
  - Short of defining a content negotiation feature for ND, not sure what we can do

# ID

# One ID type (or) Many

- The discussion seems to be converging towards having a single fixed length ID type instead of having different types
- Does the WG think that a single ID type is sufficient
  - What length should it be?
  - Should it be of a specific type (UUID, ULA etc.) or just an opaque quantity

# Metadata

- None of the drafts offer a mechanism for conveying metadata
  - E.g. Human readable name, metering, characteristics etc.
- Do we want to add such metadata?
  - If so, where?
    - The protocol documents or in the ID