# MIPv6 Base & HA Security

# Status & Issues

Jari Arkko

March 17th, 2003

Mobile IP WG meeting

IETF-56

# Presentation Outline

- Status
- Open issues

# Status

- Draft-ietf-mobileip-ipv6-21.txt
  - IETF Last Call completed, with a number of comments
  - IESG Review
    - Some comments
    - Overall looks positive so far
    - More comments coming
  - Connectathon testing has raised a few issues in the interim
- Draft-ietf-mobileip-mipv6-ha-ipsec-03.txt
  - IETF Last Call completed, with few comments
  - Will be reissued this week and sent to IESG
- Plan:
  - Resolve IESG comments
  - Resolve Connecthathon issues
  - Publish both documents as RFCs

# URLs for Issues, Statistics, Drafts

## Issues and statistics

http://www.piuha.net/~jarkko/publications/mipv6/MIPv6-Issues.html

http://www.piuha.net/~jarkko/publications/mipv6/MIPv6-Stats.html

## Drafts in text and html format

http://www.piuha.net/~jarkko/publications/mipv6/drafts/drafts.html

# Currently Discussed Issues

- 269 - Cthon: Clarify that dest BCE is not used for HOTI
- 273 - Cthon: Can a HA be CN simultaneously?
- 274 - Cthon: Send ICMPv6 PP and MH BE without BCE lookup
- 275 - Cthon: Should HA respond to NS if src = home address?
- 276 - Cthon: Sequence number example wrong
- 277 - Cthon: Should CN respond to BUs with H=1
- 278 - Cthon: Movement detection and same l-l addresses
- 279 - Cthon: NS source from HA during de-registration
- 280 - IESG review: editorial
- 281 - IESG review: technical
- 282 - IESG review: security

# 273 – Cthon: Can a HA be CN simultaneously?

- **Problem**: Can the MN send RR-based BUs to its home agent?
- Redundant home agents, one in use. Can we use RR to the others? What if we change our home agent at some stage?
- If we refuse to change H-bit in the registration, should we silently discard or return an error?
- **Proposal**: Ignore a BU with a different H-bit value than in a current BCE entry

# 277 – Cthon: Should CN respond to BUs with H=1

- **Background**: When RR is used, a BU with H=1 will be dropped.
- If a BU with H=1 is received by CN, send 131 (home registration not supported).
- **Problem**: These are in conflict at least in the following case:
  - BU, H=1
  - Both RR and IPsec used
- **Proposal**: Clarify that RR be used if and only if H=0
  - Silent discard if RR not used as expected.
  - (Similar to silent discard if IPsec policies not followed.)

# 279 – Cthon: NS source from HA during de-registration

- **Background**: A home agent might need to do a NS to send a BA to a de-registration BU.
- **Problem**: Should the MN respond to all NSs?
- Or just those from the HA while it is waiting for the BA?
- How would we know if the NS is from the HA?
  - Global / link-local address
  - Multiple addresses
- **Proposal #1**: Start answering NSes after sending the BU
  - There could be a temporary "fight" between the NAs
  - The mobile node will eventually win this contest, so it doesn't matter
  - Robust, if the home agent crashes
- **Proposal #2**: Include a PI in the NS
  - Then the MN knows its from the HA

# 281 – IESG review: Technical

- **Problem #1**: There isn't a timeout for a node marked as not supporting MH.
- **Proposal for #1**: Agreed. Specify that must timeout at some point, not do this forever. No need to specify the exact timeout.

- **Problem #2**: Clarify that multiple home addresses are possible.
- **Proposal for #2**: Agreed.

- **Problem #3**: Is the RA frequency too high?
- **Proposal for #3**: These are minimums, not defaults.

- (A few other issues included as well)

# 281 – IESG review: Security

- **Problem #1**: IKE should be a SHOULD. Related to replay protection.
- **Approach for #1**: Describe the effects and tradeoffs? Then take a new discussion with the IESG about the proper keyword.
- (A few other issues included as well)

# 278 – Cthon: Movement detection and same link-local addresses

- **Background**: Movement detection based on NUD to the router's link-local address, and observation of RAs
- **Problem**: A router might have the same link-local address on two separate links => movement not detected using the first mechanism
- **Proposal #1**: L3 movement detection is not 100% reliable and efficient anyway. Ignore the problem.
- **Proposal #2**: When a hint (L2, new RA, NUD failure) indicates a movement might have occurred, probe current router with RS. If no answer, you have moved.
- If there are no such hints and NUD works, assume the link is still good. Note: you may have moved but you will notice it upon the next RA.