# NAT Traversal for MIP – Revision (RFC 3519bis)

Sri Gundavelli (Cisco Systems)
Kent Leung (Cisco Systems)

# Motivation

- From the Implementation and deployment experience of RFC 3519, certain issues have been identified in the specification.
- There is a huge interest from the customers for deploying the NAT Traversal feature and so it is important that we fix all these issues by revising 3519.

# Issue # 1

- RFC 3344 allows the RREQ sent from the foreign agent to the home agent to use any address valid on the outgoing interface as the source address. However, RFC 3519 requires the source address of the RREQ to be the same as care-of address.

- Breaks the general assumption that the source address is the associated address of the outgoing interface. Causes issues in certain operational environments.

- (Issue 44: 3344bis Issue Tracker)

# Issue # 2

- Home Agent dependency on the source address for the NAT Detection Logic and the incompatibility with the base 3344 specification.

- SA Lookup Issue for FHAE Validation

- (Issue 45: 3344bis Issue Tracker)

# Issue # 3

- MN Registering through a Foreign Agent after receiving a FA advertisement with the ”R” bit and the issue of Non-Skippable UDP Tunnel Reply extension.

- UDP Tunnel Request extension is of skippable type, while the Tunnel Reply extension is non-skippable. Older FA versions not supporting RFC 3519 have to drop the Registration Reply, even when the tunnel is negotiated between the mobile node and the home agent. In this context, there is no need for the foreign agent to understand the UDP Tunnel Reply extension

# Issue # 4

In the scenario where the mobile node registers through a foreign agent that has sent an advertisement with the “R” bit, the protocol requires the mobile node to send a Keep-Alive message that has no protection as a control trigger for fixing the tunnel end-point settings and bringing up the tunnel.

- Leaves ample room for session hijacking

# Issue # 5

Usage of ICMP Echo Packet format for the Keep-Alive Message and the associated issues.

- There is no means to identify the user generated ICMP packets between the tunnel end points and the packets generated by the MIP system for the UDP Keep-Alive messaging. This loss of context causes implementation issues in most platforms.

# Issue # 6

Overloading the Mobile IP port 434 for control and data messages and the implementation issues

- This mixes the signaling and the data forwarding planes and collapses the routing and the MIP service functions, unlike in IP-IP and GRE encapsulation schemes where the packets are handled at the different protocol layers and the layering is preserved.

Questions ?