

# Threats to Public Multi-access IPv6 Links

(draft-ietf-ipng-netaccess-threats-00.txt)

James Kempf

DoCoMo Communications Laboratories USA

Erik Nordmark

Sun Microsystems Laboratories Europe

# The Goal

- Enumerate threats to public multi-access links
  - Examples: Ethernet, wireless Ethernet
  - Out of scope: point to point links
    - The threats don't exist on point to point links.
- RFC 2461 and RFC 2462 talk about some threats, but:
  - Superficial analysis
  - IPSEC prescribed, but may be impractical for public access networks.
- Please send your favorite threat!

# The Threats

- Threats due to Neighbor Discovery and Stateless Address Configuration.
- All but one threat are limited to nodes on the same link.
- Two classes:
  - Redirection threats (which can also be used for DoS).
  - DoS-only threats.
- Please read the draft for more details.

# The Challenge

- 802.11 in public places is becoming common.
- Fixing 802.11 security with 802.1x doesn't address the L3 threats in the draft.
- Can we come up with solutions that reduce these threats for public multi-access networks?
- For similar threats, IPv4 did not solve them.
- Fallback position is to make all public access links look like point to point links.

# Right Place for the Work

- Is the IPv6 WG interested in documenting more of these threats?
- Is the IPv6 WG interested in working on solutions?

This document was created with Win2PDF available at <http://www.daneprairie.com>.  
The unregistered version of Win2PDF is for evaluation or non-commercial use only.