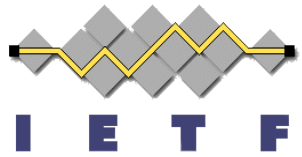
Handling ‘Rogue’ RAs

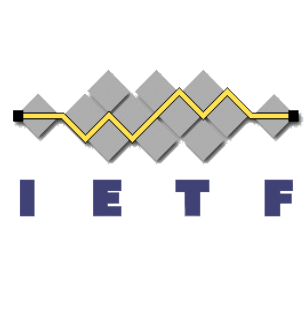
Tim Chown
tjc@ecs.soton.ac.uk



IETF 69, 23rd July 2007
Chicago

dhc WG discussion item

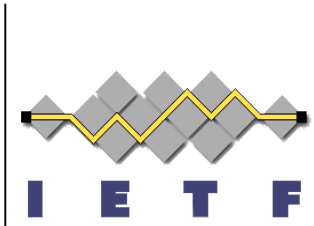
The issue



- Many enterprise network admins ask why they can't use DHCPv6 only for node autoconfiguration.
  - Generally 'comfortable' with DHCP
  - Concerned about accidental or malicious Router Advertisement misconfigurations
- They're surprised they can't get the default router address via DHCPv6

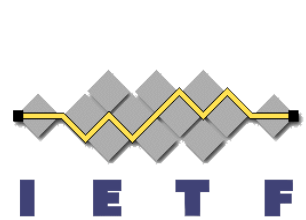
- But what's the 'rogue' RA issue?

What can cause bogus RAs?



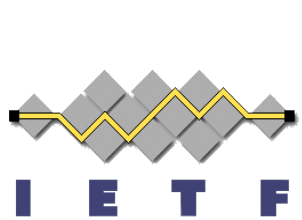
- Administrator misconfiguration
  - Directly on an interface, or perhaps by VLAN misconfiguration causing RA ‘flooding’
  - Perhaps also with a bad lifetime
- User induced accidents
  - Host acting as 6to4 router, perhaps a laptop brought in from home to work, where the laptop was a router at the home network
- Malicious
  - Some attempt to capture/redirect/etc

Some possible answers



- Manually configure the default router
- Use SeND/IPsec
- Implement RA ‘snooping’ in switches
- Add some RIP-like password option
- Use router preference option
- Use L2 admission control (e.g. 802.1x)
- Use host-based packet filters
- Use some auto-deprecate tool
- Make it harder to accidentally be a 6to4 router
- **Enhance DHCPv6 to add default router support**

Thoughts?



- Some solutions help against some types of RA problems
- Those using DHCP now invariably don't use authenticated DHCP
- Enhancing DHCPv6 would be quite a fundamental change
  - A lot more to consider beyond adding a default router option
- We should probably check behaviour of deprecating rogue RA information
- This is an issue that is being quite commonly raised, so consensus on practical solutions/advice is desirable.