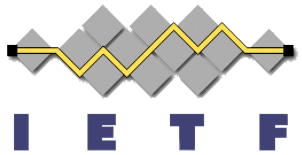
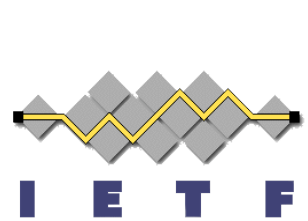
IPv6 Implications for Network Scanning

Tim Chown
tjc@ecs.soton.ac.uk



IETF 67, November 6th, 2006
San Diego, CA

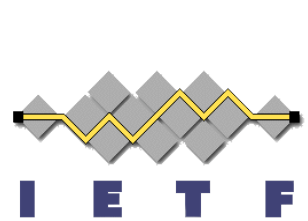
Status



- This is a revised -01 WG draft
  - Previously three personal draft instances
  - Each revised with WG feedback

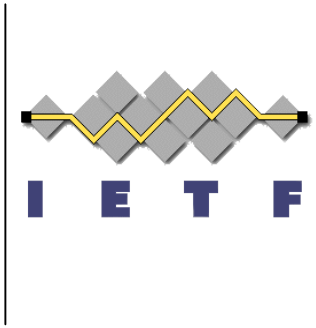
- Referenced in two mature v6ops drafts
  - NAP
    - draft-ietf-v6ops-nap-04
  - ICMP filtering
    - draft-ietf-v6ops-icmpv6-filtering-recs-02

Goals of the document



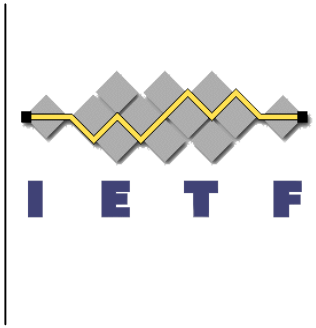
- Note the properties of the vastly increased host address space in an IPv6 subnet (/64) or site (/48)
  - With respect to traditional network scanning probes or worms as seen today for IPv4 networks
- Describe new methods that attackers may use to locate nodes for further exploitation
  - Given the target host address space is so large
- Make suggestions to administrators to mitigate against the new attack methods
- Publish as Informational

Changes since -00



- Emphasis on Informational nature
- Discussed ‘law of diminishing returns’ and where ‘address hiding’ fits into the security model
- Added Bellovin’s worm paper reference
- Suggested avoiding any repeated host numbering patterns, not just sequential
- Added note on two-faced DNS
- Added note on reverse DNS disclosure
- Added note on Embedded-RP/RFC3306 disclosure
- Added note on application-specific addresses

Next steps?



- Have addressed comments in -01
  - Now had one revision/update as a WG item
- Is there any more to add to the document?
  - Is it worth publishing?
  - If not, what to do with the two referring mature drafts?
  - If so, is it ready for a last call on the -01?
- Comments?