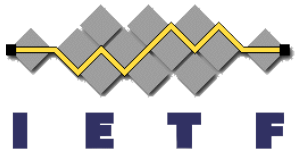
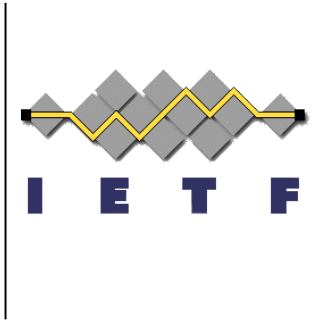
Operational Security Considerations for IPv6 Networks

K. Chittimaneni, M. Kaeo, E. Vyncke



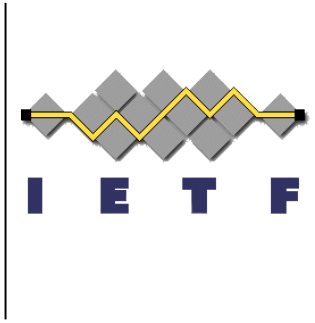
IETF 86, March 14 2013
Orlando, Florida

Updates for -02



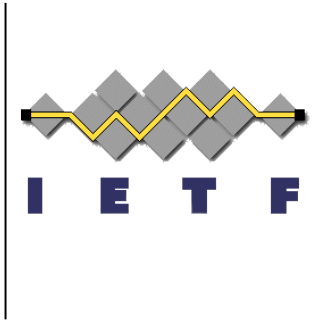
- 2.1.2 Use of ULAs
  - Point out that using /32 ULAs violates RFC 4193 and greatly reduces the probability of non-collisions between ULA prefixes
  - Reference RFC 4864
  - Point out that ULAs are supposed to be used in conjunction with global addresses for hosts that desire external connectivity but some operators chose to use ULAs with some sort of address translation at the border in order to maintain a perception of parity between their IPv4 andIPv6 setup
  - NPT wording clarified
  - Clarified paragraph discussing BGP filters and that using ULA does not prevent route and packet filters to be implemented and monitored

Updates for -02



- 2.1.3 Point-to-Point Links
  - Referenced RFC 6164 and recommended use of /127s
- 2.1.4 Privacy Extension Addresses
  - Use terminology of Temporary Addresses
  - Point to other works describing this in detail
  - Point out that it is advised in scenarios where attribution is important to disable stateless address auto configuration and rely only on DHCPv6. However, in scenarios where anonymity is a strong desire, temporary addresses should be used

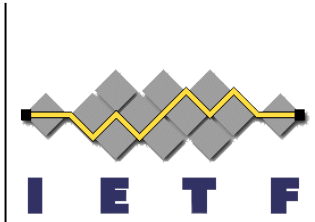
Updates for -02



- 2.3.3 Packet Exceptions
  - Removed expired reference
  - Added draft-6man-oversized-header-chain reference
- 2.6.2 Transition Mechanisms
  - Added more details on what could be blocked for tunneling mechanisms
  - Change text for 6to4 section to accurately reflect that client usage of 6to4 by default is now discouraged, and significant precautions are needed to avoid operational problems [RFC6343]

ToDo

- Final wg review – ready for Last Call?
- Contact us at opsec@ietf.org



Q&A

THANK YOU!