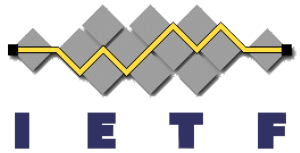
Operational Security Considerations for IPv6 Networks

K. Chittimaneni, E. Vyncke, M. Kaeo

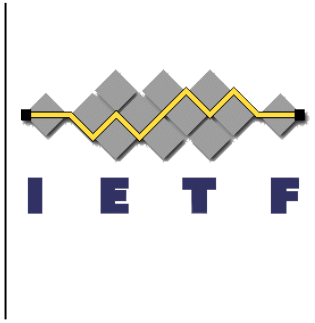


IETF 84, August 1 2012,
Vancouver, Canada

Updates to -01

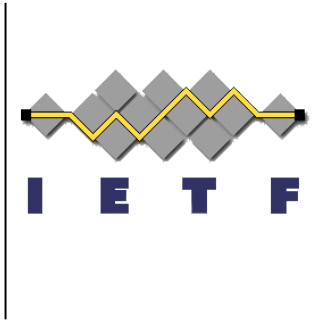
- Filled in missing text
  - Addressing Architecture
    - Overall Structure
    - ULAs
    - Point-to-Point Links
    - Privacy Addresses
  - Enterprise Security Considerations
- Update references

Mailing List Comments



- 2.1.1 Addressing Structure
  - Clarify that some devices typically have addresses manually configured and not encourage manually configured addresses
- 2.1.2 ULAs
  - Include that ULAs make troubleshooting difficult
- 2.1.3 Point-to-Point Links
  - reference draft-ietf-v6ops-v6nd-problems,since using /112 also works as a workaround for buggy implementations that fail to properly manage the Neighbor Cache
- 2.1.4 Privacy Addresses
  - mention draft-gont-opsec-ipv6-host-scanning that explains some concerns even when using DHCPv6 or privacy addresses
- 2.2 Link Layer Security
  - mention ND cache DoS concerns and protection

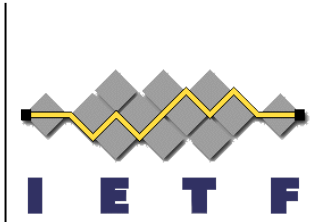
Mailing List Comments (2)



- 2.2.1 SeND and CGA
  - mention the limitation of vendor support that makes SeND challenging to deploy widely
- 2.3 Control Plane Security
  - mention rate-limiting of the valid packets should be done for Mgmnt and Control Plane.
- 2.6.3.1 Carrier Grade Nat (CGN)
  - mention the log size concern and draft-donley-behave-deterministic-cgn
- 3.1 External Security Considerations
  - mention “Implement Anti-Spoof filtering or other Anti-Spoof protections”. Anti-Spoof filtering could be ACLs. But RTBH could also be implemented if BGP is used on the CPE
- 3.2 Internal Security Considerations
  - mention “filtering IPv6 Tunneling that can bypass outbound security policy” (the usual Torrent over Teredo tunnel example in Section 5)

ToDo

- Request adoption as working group item
- Next pass to fill in rest of gaps
- Continue to work with v6ops and homenet WGs to avoid overlaps or conflicts
- Contact us at opsec@ietf.org



Q&A

THANK YOU!