Teredo Security Updates

draft-krishnan-v6ops-teredo-update-03.txt

Dave Thaler

Suresh Krishnan

Jim Hoagland

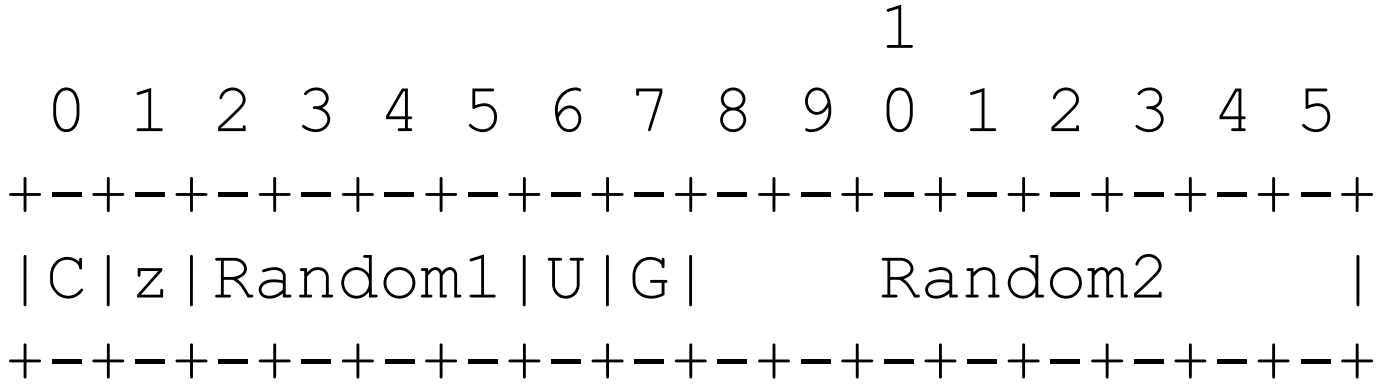
Status

- Draft specifies what is already deployed
  - (Vista, Windows Server 2008, any others?)
- Addressed previous feedback
  - Replaced normative text with relevant text from MS-TERE
- Added Dave Thaler as co-author

- Note well: Teredo has an IPR declaration from Microsoft (RAND-Z for any standards track docs)
  - http://www.ietf.org/ietf/IPR/microsoft-ipr-draft-huitema-v6ops-teredo.txt
  - This should apply to the 2 Teredo drafts too
  - Updated declaration is in progress

Random Address Flags

- Goal: Make guessing IPv6 address harder than just guessing external IPv4 addr/port



- **Random1,Random2:** MUST be set to a random value (previously MUST be zero)
- **z,U,G:** as specified in [RFC4380]

Deprecation of Cone Bit

- Goal: Avoid telling potential attackers that your NAT is a cone NAT (C bit)
- Effect of C=0 is that extra signaling messages will be sent via the Teredo server
- Ignoring C bit (just sending the extra messages) is already allowed in [RFC4380] section 5.2.4
- Deprecating C bit simply forces that behavior
  - SHOULD just set C=0
  - SHOULD treat peers as if C==0
- Additional bonuses:
  - The initial NAT-determination process gets faster (IPv6 “comes up” sooner)
  - Teredo gets more reliable since some cone NATs aren’t cone in some cases (port preservation fails)

Security Considerations

- “Teredo is NOT RECOMMENDED as a solution for managed networks. Administrators of such networks may wish to filter all Teredo traffic at the boundaries of their networks.”

- Note in Implementation Status Appendix:
  - “All Windows implementations automatically disable Teredo if they detect that they are on a managed network with a domain controller.”