GRE-in-UDP Encapsulation

draft-ietf-tsvwg-gre-in-udp-06

Tom Herbert

March 2015 Dallas, USA

Progress Since Hawaii

- MPLS/UDP draft is complete and headed to RFC publication
  - Many thanks to David Black, Routing/TSV ADs' efforts
  - Some technical areas apply to both MPLS/UDP and GRE/UDP
  - This version adapts solutions from the MPLS/UDP draft
- Updated topics in GRE/UDP draft
  - Congestion considerations
  - UDP zero-checksums in IPv6
  - Security
  - UDP source port value
  - Many editorial changes in latest version

Congestion Considerations

- Congestion-controlled traffic
  - Not a problem
  - IP traffic assumed to be congestion controlled
- Otherwise (not congestion controlled, or not known to be congestion controlled)
  - Service provider or cooperating providers
    - Careful provisioning by network operator(s) (MUST)
    - Prevent uncontrolled traffic from “escaping” (SHOULD)
  - No general/public Internet usage (MUST NOT)

IPv6 UDP Zero-Checksums

- Issue: No IPv6 header checksum
  - Rely on link and/or UDP checksums
  - Between links: UDP checksum only
- IPv6 UDP zero checksum usage conditions
  - Under single administrator where packet corruption is known to be exceptionally unlikely
  - Under single administrator where observational measurement indicates low likelihood of corruption
  - Applications are tolerant of packet corruption

IPv6 UDP Zero-Checksums

- Protocol design to meet [RFC6935] and [RFC6936]
  - A) UDP checksum with IPv6 MUST be the default
  - D) an encapsulator SHOULD use different IPv6 addresses for each GRE-in-UDP tunnel that uses UDP zero-checksum mode
  - F) Measure SHOULD be taken to prevent Ipv6 traffic with zero UDP checksum from “escaping” to Internet
  - G) IPv6 traffic with zero UDP checksums MUST be actively monitored for errors by the network operator
  - Additional B), H)
  - Not adopting “c. the tunel decapsulator SHOULD only allow the use of UDP zero-checksum mode for IPv6 on a single received UDP Destination Port regardless of the encapsulator” from MPLS/UDP

Security

- GRE/UDP encapsulation does not secure payload
  - DTLS [RFC6347] can be used for application security
    - Single DTLS session for any specific tunnel
    - DTLS tunnel only supports unicast traffic
    - DTLS tunnel is subject to meet IPv6 UDP zero checksum requirements (Section 5.2)
- Concerns of corruption of GRE header
  - Issue when GRE key is used for segmentation (e.g. NVGRE)
  - Either UDP checksum or GRE checksum SHOULD be used.
    - In particular, when IPv6 UDP zero-checksums mode is used, GRE checksum SHOULD be used

UDP Source Port Value Setting

- The port can hold a 16-bit entropy value
  - Refers to encapsulated flow
  - Value SHOULD be in ephemeral port range (i.e. 14 bits)
  - Selected port value can change during lifetime of a flow
- If a value cannot be derived from packet
  - Set port to a randomly selected constant value to avoid packet reordering in flows
  - Change random value periodically to mitigate DoS attack

Other Editing Changes

- Change the title to GRE-in-UDP encapsulation (was: Generic UDP encapsulation in IP Tunneling)
- Reorder the sections for better flow
- Refer to [RFC5405bis] as a requirement check-list
- Modify the text in applicability statement (Section 1.1)
- Modify the text for UDP checksum with IPv4
- Add Tom Herbert as co-author and Gorry Fairhust as a contributor

Next Steps

- Address additional comments/feedback on this version
  - Any remaining technical concerns?
- Seek WG LC in mid of this year