UDP Encapsulation for IP Tunneling

draft-yong-tsvwg-udp-4-ip-tunneling-01

Lucy Yong, Xiaohu Xu

March 2013  Orlando FL
Background

• IP Infrastructure Networks carry tunneled traffic
  – Transit nodes are not aware of tunneled traffic/protocols
  – Tunneled traffic may be IP or non-IP packets

• IP Networks are built on parallelized capacity
  – Operator’s desire to use all the paths carrying the tunneled traffic

• IP Networks already support ECMP and LAG
  – Hashing based load distribution is the common practice
    • IP header and TCP/UDP header are used for ECMP load distribution
    • packets with the same five tuple is carried on the same path, which ensures no packet re-ordering
    • UDP src and dst ports are used as entropy in the load distribution
Problem Statement

• Tunneled traffic may be carried over IP network where ECMP/LAG is required
  – To avoid tunneled flow packets re-ordering, IP network MUST keep a tunneled flow in the same path
    • The way to address this is to have an entropy field in packets for IP network with ECMP, in which a tunneled flow packets is assigned to the same entropy value

• Existing solution weakness for IP network with ECMP
  – IP-in-IP [RFC2003] does not have a place for entropy info
  – GRE [RFC2784] has an entropy field but requires transit router special processing
  – L2TPv3 [RFC3931] has the same capability and problem as GRE
What is in this draft?

• Specify a generic UDP encapsulation method for any tunneled layer protocol over IP networks w/ ECMP
  – Achieve it w/o any change in IP network transit nodes
    • the same LB method for both host based apps. and tunneled apps.
  – Have a flow entropy field in UDP header
    • UDP src and dst ports are commonly used as entropy in IP network
    • tunneled packets w/ the same entropy value carried through the same path in IP network
      • may map one or more tunneled flows to the same value
  – Have a way to identify tunneled protocol in the UDP header
    • needed in order to support any tunneled layer protocol

• Specify tunnel endpoint process procedures and error handling
UDP Encapsulation for IP Tunneling

- UDP source port is used as the flow entropy field
  - may be set to any value by the tunnel ingress
  - Varying the value according to the payload flow will enable load balancing within IP networks
- UDP destination port is set to indicate the tunneled layer protocol that is registered under IANA
- Other UDP header fields remain the same as in [RFC768]
- RECOMMEND that the UDP checksum field is set to zero.
UDP Header Usage in this draft

• UDP port usage here is different from before
  – Not for demultiplexing transport connection at end point
  – Nor identifying an upper layer service

• Header does not provide transport function for any upper layer application

• UDP ports are to provide flow entropy and indication of tunneled protocol type
  – the ports have been used as entropy in IP network
  – the latter is necessary for egress

**Note:** VXLAN have been implemented in this way
Next Steps

• Welcome comment and feedback on this
• Address comments and feedback
• Upload next version