



IPv6/UDP Zero-Checksum

Magnus Westerlund

Gorry Fairhurst

draft-fairhurst-tsvwg-6man-udpzero-02

Why are we discussing this

- › Different Tunnels have implementation issues:
 - IPv6 tunnels that want ECMP using UDP
 - **Automatic IP Multicast Without Explicit Tunnels (AMT)** (draft-ietf-mboned-auto-multicast)
 - **Locator/ID Separation Protocol (LISP)** draft-ietf-lisp
- › RFC 2460 mandates a non-zero IPv6 Checksum
- › Implementers want to avoid having to checksum the UDP payload

IPv6 Transport

- › IPv6 lacks header checksum, relying on transport protocol for delivery verification at destination
- › Need to verify the src,dst address, src,dst ports, and start of payload
- › Many UDP applications don't know how to check this themselves

Many accept from any source address and port

Corruption of the header poses a real problem if undetected



UDP Tunnels

- › UDP checksum provides protection
- › UDP-Lite protects header information

- › Many tunnel applications rely on the inner tunneled packet being checked at the final destination
 - Therefore there is a claim that no checksum is needed
 - IPv4 tunnels typically uses UDP with zero checksum
 - Supported in currently deployed hardware
 - Implementers therefore want the same functions for IPv6



This is not trivial

- › draft-fairhurst-tsvwg-6man-udpzero-02 describes key issues and pitfalls

- › UDP-Lite would be a candidate transport

- › If the group really wants to consider whether to relax the UDP checksum coverage for the tunnel case:
 - Zero checksums should be explicitly enabled for a specific port
 - The tunnel must not fragment packets
 - The tunnelled packet must provide integrity checks
 - Protocols than use zero checksum must not be tunneled themselves
 - etc

What to do

1. This draft provides a basis for making a decision about whether to update RFC 2460.
2. We should publish a document on this topic – whichever way the decision goes!
3. Can we adopt this as a Working Group item?

Extra Slides

Corruption

