Automatic Multicast Tunneling

draft-ietf-mboned-auto-multicast-12

IETF 83 – Paris, France
Summary

• Document Status
• Document Changes
• Protocol Changes
• Outstanding Issues
• Next Steps
Document Status

• Document reorganized, reformatted, re-worded, rewritten and expanded.
• Document distributed for a pre-submission review.
• Document updated to reflect feedback.
• Submitted for publication as Draft 12 in February.
Document Changes

• Primary rationale for changes:
  – To satisfy current IETF Editor guidelines and current practice, with the goal of ensure smooth passage through the RFC approval process.
  – To shift focus of document to that of implementation.
  – To add informative content to provide a context for describing normative requirements.
  – Provide greater detail as required to eliminate ambiguities and and address those areas that were lacking definition.
Document Changes (cont)

• Document split into informative and normative sections.

• High-level Organization:
  – Protocol Overview (Informative)
    • General Architecture
    • General Operation
  – Protocol Description (Normative)
    • Message Formats
    • Gateway Operation
    • Relay Operation
Document Changes (cont)

• Renewed emphasis on AMT as a simple encapsulation protocol for exchanging IGMP/MLD messages and multicast data generated “outside” of the protocol.

• Group subscription management and multicast forwarding are considered external activities that feed into AMT.

• These activities are governed by the IGMPv3 and MLDv2 specifications.

• The Request->Membership Query exchange is a mechanism for generating general queries.
Relationship to Host IP Stack
Document Changes (cont)

• Treat relay discovery as a distinct feature of the protocol.
  – Use of the discovery mechanism is optional.
  – Gateway implementations may use alternative methods for discovery.
  – Mention possible requirement for source-specific discovery. Use of global anycast address may return relay without multicast connectivity to desired sources.
Protocol Changes

• Backwards compatible.
• Request “Protocol” or “P” flag
  – Indicate to relay whether it should return IGMPv3 or MLDv2 general query in Membership Query message.
• Membership Query “Limit” or “L” flag
  – Notifies gateway that the relay is NOT accepting Membership Update messages from new gateway tunnel endpoints.
  – Typically set when anycast address prefix advertisement has been withdrawn (if applicable).
Outstanding Issues

• Source address in IGMP/MLD packet headers.
• UDP Checksums in outer-headers.
• Global Anycast Address Prefix Allocation
Source Address in IGMP/MLD Packets

• Both protocols expect link-local addresses.
• IGMP allows for use of the unspecified (0.0.0.0) address as a source address. Hosts and routers accept these messages.
• MLD Does not! Hosts and routers must ignore MLD packets that carry an unspecified source address.
Link-Local Addresses for IGMP/MLD

• If MLD does not allow use of an unspecified source address, what should gateways and relay insert into the message headers?

• Does implementation rely on existing host IP/MLD stack for message processing?
  – If no, then just ignore it.
  – If yes, then
    • Spec simply indicates that recipient may need to regenerate message with valid link-local address.
    • Where does that come from? Assign special prefix and addresses for AMT virtual/pseudo interfaces?
UDP Checksum Issue

• Overview
  – AMT uses UDP encapsulation.
  – Relays will use existing functionality to encapsulate multicast packets into Multicast Data messages.
  – The encapsulation functionality provided by many platforms cannot generate a valid UDP checksum for the outer UDP header.
  – Workaround for IPv4 is to set checksum to zero.
  – This will not work for current IPv6 as that protocol specification explicitly prohibits the use of zero-checksums.
  – Workaround for IPv6 is to relax requirements.

• Detailed description of problem may be found in:
  – draft-ietf-6man-udpchecksums
  – draft-ietf-6man-udpzero
UDP Checksums and AMT

• Control messages are not a problem.
• Data messages are.
• What impact does this have on AMT?
  – Gateway that relies on host IP stack stack implementation cannot control handling unless API is provided.
  – Gateway that operates below or bypasses the IP stack MUST accept Multicast Data messages with zero UDP checksums.
UDP Checksums and AMT (cont)

• How to detect when zero-checksum packets are dropped?
  – Add some form of Keep-Alive/Beacon functionality. Relay periodically sends packets with and without zero-checksums.
UDP Checksums and AMT (cont)

• Use different discovery address to locate nearest relay that does compute checksums.
  • Result may reduce/eliminate benefits provided by that does compute checksums.
  • Result may reduce/eliminate benefits provided by

• Flags may be added to Relay Discovery and Relay Advertisement message to negotiate switch to IPv4.

• Flags may be added to Relay Discovery and Relay Advertisement message to negotiate switch to IPv4.
Next Steps

are required, complete those ASAP (like next week).

• Review changes. Enlist reviewers today.
• Submit Draft 13.

• Start process of advancing the document through the RFC approval process (chairs an AD)