MBoneD Working Group
Internet Engineering Task Force
INTERNET-DRAFT
17 February 1999
Expires August 1999

Mark Handley
ISI
Dave Thaler
Microsoft
Roger Kermode
Motorola

Multicast-Scope Zone Announcement Protocol (MZAP)
<draft-ietf-mboned-mzap-03.txt>

Status of this Memo

Abstract

This document defines a protocol, the Multicast-Scope Zone Announcement Protocol (MZAP), for discovering the multicast administrative scope zones that are relevant at a particular location. MZAP also provides mechanisms whereby two common misconfigurations of administrative scope zones can be discovered.

Copyright Notice

1. Introduction

IP Multicast groups can be of global scope, or they can be restricted in scope using a scoping mechanism. In this document, we only consider administrative scoping, as defined in RFC 2365 [1]. An administrative scope zone is defined by a set of routers surrounding a region of the network. These "border routers" are configured to not pass multicast traffic destined for a particular range of multicast addresses to or from links leaving the scope zone.

Administrative scope zones may be of any size, and a particular host may be within many administrative scope zones of various sizes. The only zones a host can assume that it is within are the global zone, and a "Local Scope". A Local Scope is defined as being the smallest administrative scope zone encompassing a host, and the border is configured for addresses in the range 239.255.0.0 to 239.255.255.255 inclusive. RFC 2365 specifies:

> "239.255.0.0/16 is defined to be the IPv4 Local Scope. The Local Scope is the minimal enclosing scope, and hence is not further divisible. Although the exact extent of a Local Scope is site dependent, locally scoped regions must obey certain topological constraints. In particular, a Local Scope must not span any other scope boundary. Further, a Local Scope must be completely contained within or equal to any larger scope. In the event that scope regions overlap in area, the area of overlap must be in its own Local Scope. This implies that any scope boundary is also a boundary for the Local Scope."

as well as:

> "administrative scopes that intersect topologically should not intersect in address range."

Two problems make administrative scoping difficult to deploy and difficult to use:

- Misconfiguration is easy. It is difficult to detect scope zones that have been configured so as to not be convex (the shortest path between two nodes within the zone passes outside the zone), or to leak (one or more border routers were not configured correctly), or to intersect in both area and address range.

- Applications have no way to discover the scope zones that are relevant to them. This makes it difficult to use administrative scope zones, and hence reduces the incentive to deploy them.

This document defines the Multicast Scope Zone Announcement Protocol (MZAP) which will provide applications with information about the scope zones they are within, and also provide diagnostic information to detect misconfigured scope zones.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [2].

Constants used by this protocol are shown as [NAME-OF-CONSTANT], and summarized in section 5.

2. Overview

A multicast scope Zone Border Router (ZBR) is a router that is configured to be a zone border on one or more of its interfaces. Any interface that is configured to be a border for any administrative scope zone MUST also be a border for the Local Scope zone, as defined in [1].

Routers SHOULD be configured so that the router itself is within the scope zone. This is should in figure 1(a), where router A is inside the scope zone and has the border configuration. It is possible for the first router outside the scope zone to be configured with the border, as illustrated in figure 1(b) where routers B and C are outside the zone and have the border configuration, but this is NOT RECOMMENDED.

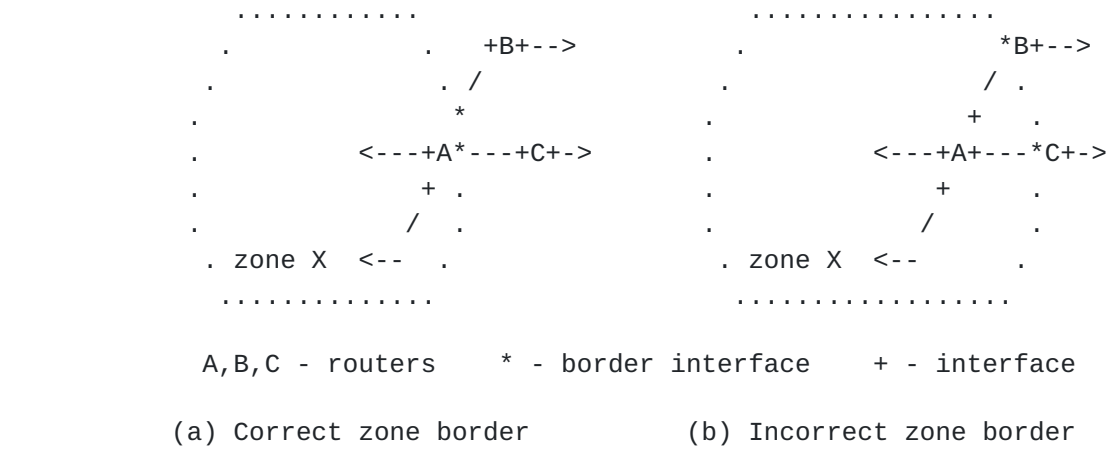


Figure 1: Administrative scope zone border placement

This rule does not apply for Local Scope borders, but applies for all other administrative scope border routers.

When a ZBR is configured correctly, it can deduce which side of the boundary is inside the scope zone and which side is outside it. It can also send messages into the scope zone, which it SHOULD NOT be able to do if the router itself is considered outside the scope zone.

Such a ZBR should then send periodic Zone Announcement Messages (ZAMs) for the zone for which it is configured as a border from one of its interfaces that go into that scope zone. These messages are multicast to the address [MZAP-LOCAL-GROUP] in the Local Scope.

Each ZBR also listens for messages from other ZBRs for the same border. The ZBR with the lowest interface IP address within the zone from those ZBRs forming the zone border becomes the zone-id router for the zone. The combination of this IP address and the first multicast address in the scoped range serve to uniquely identify the scope zone.

When a ZBR receives a ZAM for some scope zone:

- If the ZAM was received on an interface with a boundary for the given scope, the ZAM is not forwarded. For example, router D in figure 2 will not forward the ZAM.

- If the ZAM was received on an interface which is NOT a Local Scope boundary, and the last Local Zone ID Address in the path list is 0, the ZBR fills in the Local Zone ID Address of the local zone from which the ZAM was received.

- If a ZAM for the same scope (as identified by the origin Zone ID and first multicast address) was received in the last [ZAM-DUP-TIME] seconds, the ZAM is not forwarded. For example, when router C in figure 2 receives the ZAM via B, it will not be forwarded, since it has just forwarded the ZAM from E.

- Otherwise, the ZAM is cached for at least [ZAM-DUP-TIME] seconds.

- If the Zone ID of the Local Scope zone in which the ZBR resides is not already in the ZAM's path list, then the ZAM is immediately re-originated within the Local Scope zone. It adds its own address and the zone-id of the Local Scope zone into which the message is being forwarded to the ZAM path list before doing so. A ZBR receiving a ZAM with a non-null path list MUST NOT forward that ZAM back into a Local Scope zone that is contained in the path list. For example, in figure 2, router F, which did not get the ZAM via A due to packet loss, will not forward the ZAM from B back into Zone 2 since the path list has { (E,1), (A,2), (B,3) } and hence Zone 2 already appears.

o In addition, the ZBR re-originates the ZAM out each interface with a Local Scope boundary (except that it is not sent back out the interface over which it was received, nor is it sent into any local scope zone whose ID is known and appears in the path list). In each such ZAM re-originated, the ZBR adds its own IP address to the path list, as well as the Zone ID Address of the Local Scope Zone into which the ZAM is being sent, or 0 if the ID is unknown. (For example, if the other end of a point-to-point link also has a boundary on the interface, then the link has no Local Scope Zone ID.)

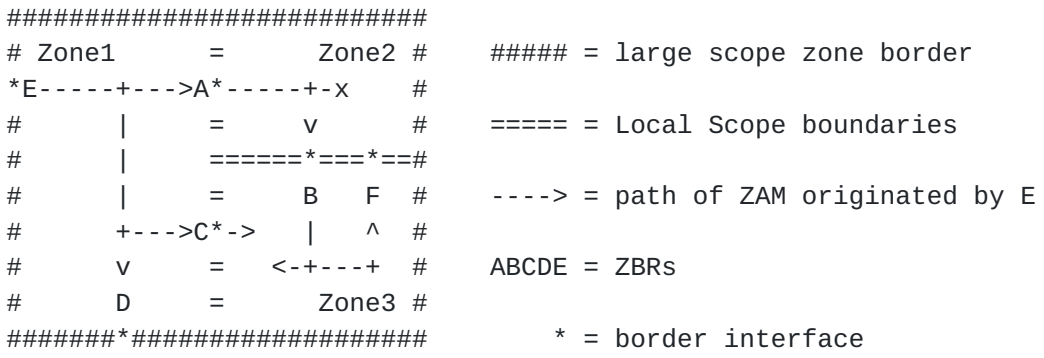


Figure 2: ZAM Flooding Example

The packet also contains a Zones Traveled Limit. If the number of Local Zone IDs in the ZAM path becomes equal to the Zones Traveled Limit, the packet should be dropped. Zones Traveled Limit is set when the packet is first sent, and defaults to 32, but can be set to a lower value if a network administrator knows the expected size of the zone.

Additional messages called Zone Convexity Messages (ZCMs) SHOULD also be sent to the [ZCM-RELATIVE-GROUP] in the scoped range itself. As these are not locally scoped packets, they are simply multicast across the scope zone itself, and require no path to be built up, nor any special processing by Local Scope zone ZBRs. These messages are used to detect non-convex administrative scope zones, as illustrated in figure 3, where the path between B and D goes outside the scope (through A and E). Here Router B and Router C originates ZCMs, each reporting each other's presence. Router D cannot see Router B's messages, but can see C's report of B, and so can conclude the zone is not convex.

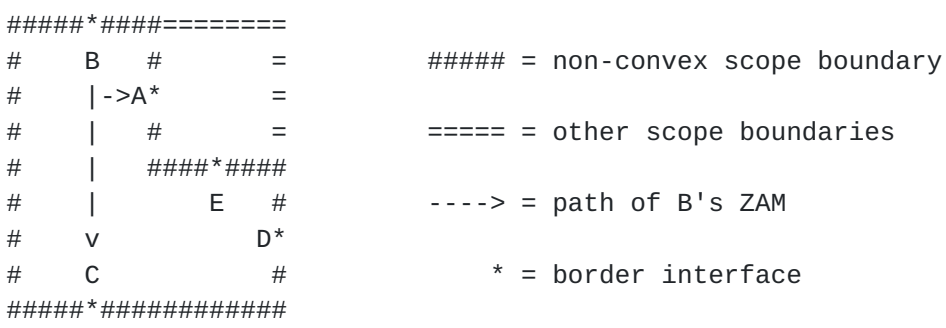


Figure 3: Non-convexity detection

2.1. Nesting

MZAP also provides the ability to discover the nesting relationships between scope zones. Two zones are nested if one is comprised of a subset of the routers in the other, as shown in Figure 4.

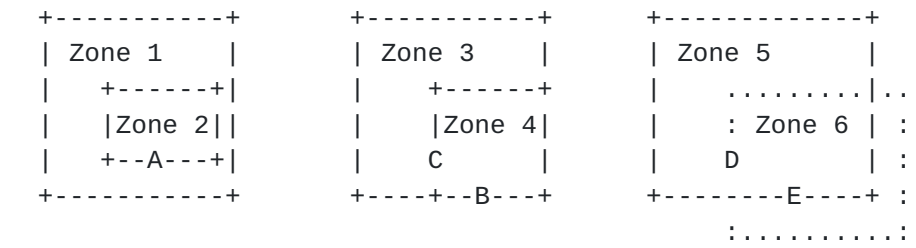


Figure 4: Zone nesting examples

Nested scopes provide the ability to perform "expanding-scope" searches in a similar, but better behaved, manner to the well-known expanding ring search where the TTL of a query is steadily increased until a replier can be found. Studies have also shown that nested scopes can be useful in localizing multicast repair traffic [8].

A ZBR cannot independently determine whether one zone is nested inside another. However, they can determine that one zone does NOT nest inside another. For example, in figure 4:

- ZBR A will pass ZAMs for zone 1 but will prevent ZAMs from zone 2 from leaving zone 2. ZBR A can thus determine that zone 1 does not nest within zone 2, but it cannot, however, determine whether zone 2 nests within zone 1.

- ZBR B acts as ZBR for both zones 3 and 4, and hence cannot determine if one is nested inside the other. However, ZBR C can determine that zone 3 does not nest inside zone 4 since it is a ZBR for zone 4 and not zone 3.

- ZBR D only acts as ZBR zone 6 and not 5, hence ZBR D can deduce that zone 6 does not nest inside zone 5. Similarly, ZBR E only acts as ZBR zone 5 and not 6, hence ZBR E can deduce that zone 5 does not nest inside zone 6.

The fact that ZBRs can determine that one zone does not nest inside another, but not that a zone does nest inside another, means that nesting must be determined in a distributed fashion.

When a ZBR receives a ZAM for a scope X for which it is NOT a border, it creates a local "X not inside" state entry, if such an entry does not already exist. It then restarts the entry's timer at [ZAM-HOLDTIME]. Existence of this state indicates that the ZBR knows that X does not nest inside any scope for which it is a border. If the entry's timer expires (because no more ZAMs for X are heard for [ZAM-HOLDTIME]), the entry is deleted.

Periodically, at an interval of [NIM-INTERVAL], a router originates a Not-Inside Message (NIM) for each "X not inside" entry, for each scope zone Y for which it is a border. Like a ZAM, this message is multicast to the address [MZAP-LOCAL-GROUP] from one of its interfaces in Y.

When a ZBR receives a NIM saying that "X is not inside Y", it is forwarded, unmodified, in a manner similar to ZAMs:

- If the NIM was received on an interface with a boundary for either X or Y, the NIM is discarded.

- Unlike ZAMs, if the NIM was not received on the interface towards the message origin (according to the Multicast RIB), the NIM is discarded.

- If a NIM for the same X and Y (where each is identified by its first multicast address) was received in the last [ZAM-DUP-TIME] seconds, the NIM is not forwarded.

- Otherwise, the NIM is cached for at least [ZAM-DUP-TIME] seconds.

- The ZBR then re-originates the NIM (unchanged) into each local scope zone in which it has interfaces, except that it is not sent back into the local scope zone from which the message was received, nor is it sent out any interface with a boundary for either X or Y.

3. Usage

In this section, we summarize how to inform internal entities of scopes in which they reside, as well as how to detect various error conditions. If any error is detected, the router should attempt to alert a network administrator to the nature of the misconfiguration. The means to do this lies outside the scope of MZAP.

3.1. Zone IDs

When a border router first starts up, it uses its lowest IP address which it considers to be inside a given zone as the Zone ID for that zone, and schedules the ZCM and ZAM messages to be sent in the future (it does not send them immediately). When a ZAM or ZCM is received for the given scope, the sender is added to the local list of ZBRs (including itself) for that scope, and the Zone ID is updated to be the lowest IP address in the list. Entries in the list are eventually timed out if no further messages are received from that ZBR, such that the Zone ID will converge to the lowest address of any active ZBR for the scope.

3.2. Informing internal entities of scopes

Any host or application may join the [MZAP-LOCAL-GROUP] to listen for Zone Announcement Messages to build up a list of the scope zones that are relevant locally, and for Not-Inside Messages if it wishes to learn nesting information. However, listening for to such messages is not the recommended method for regular applications to discover this information. These applications will normally query a local Multicast Address Allocation Server [3], which in turn listens to Zone Announcement Messages and Not-Inside Messages to maintain scope information.

An internal entity may assume that X nests within Y if:

a) it first heard ZAMs for both X and Y at least [NIM-HOLDTIME] seconds ago, AND

b) it has not heard a NIM indicating that "X not inside Y" for at least [NIM-HOLDTIME] seconds.

3.3. Detecting non-convex scope zones

Non-convex scope zones can be detected via two methods:

(1) If a ZBR is listed in ZCMs received, but the next-hop interface (according to the multicast RIB) towards that ZBR is outside the scope zone, or

(2) If a ZBR is listed in ZCMs received, but no ZCM is received from that ZBR for [ZCM-HOLDTIME] seconds, as illustrated in figure 3.

Zone Convexity Messages MAY also be sent and received by correctly configured ordinary hosts within a scope region, which may be a useful diagnostic facility that does not require privileged access.

3.4. Detecting leaky boundaries for non-local scopes

Leaky scope boundaries can be detected via two methods:

(1) If it receives ZAMs originating inside the scope boundary on an interface that points outside the zone boundary. Such a ZAM message must have escaped the zone through a leak, and flooded back around behind the boundary. This is illustrated in Figure 5.

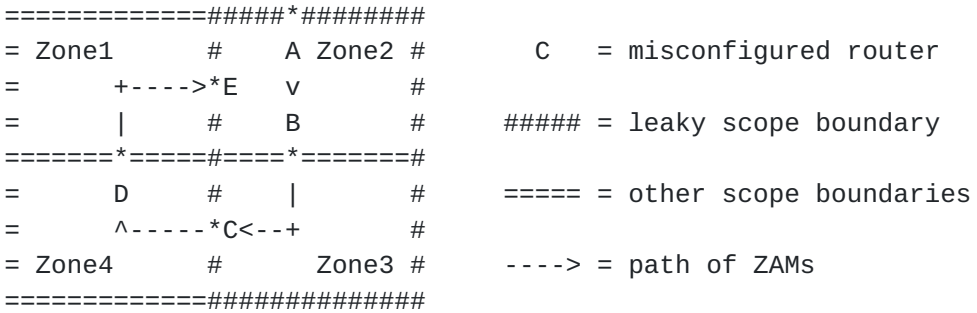


Figure 5: ZAM Leaking

(2) If a ZLE message is received.

In either case, the misconfigured router will be either the message origin, or one of the routers in the path list included in the message received.

3.5. Detecting a leaky Local Scope zone

A local scope is leaky if a router has an administrative scope boundary on some interface, but does not have a Local Scope boundary on that interface as specified in RFC 2365. This can be detected via the following method:

- If a ZAM for a given scope is received by a ZBR which is a border for that scope, it compares the Origin's Scope Zone ID in the ZAM with its own Zone ID for the given scope. If the two do not match, this is evidence of a misconfiguration. Since a temporary mismatch may result immediately after a recent change in the reachability of the lowest-addressed ZBR, misconfiguration should be assumed only if the mismatch is persistent.

The exact location of the problem can be found by doing an mtrace [5] from the router detecting the problem, back to the ZAM origin, for any group within the address range identified by the ZAM. The router at fault will be the one reporting that a boundary was reached.

3.6. Detecting conflicting scope zones

Conflicting address ranges can be detected via the following method:

- If a ZBR receives a ZAM for a given scope, and the included start and end addresses overlap with, but are not identical to, the start and end addresses of a locally-configured scope.

Conflicting scope names can be detected via the following method:

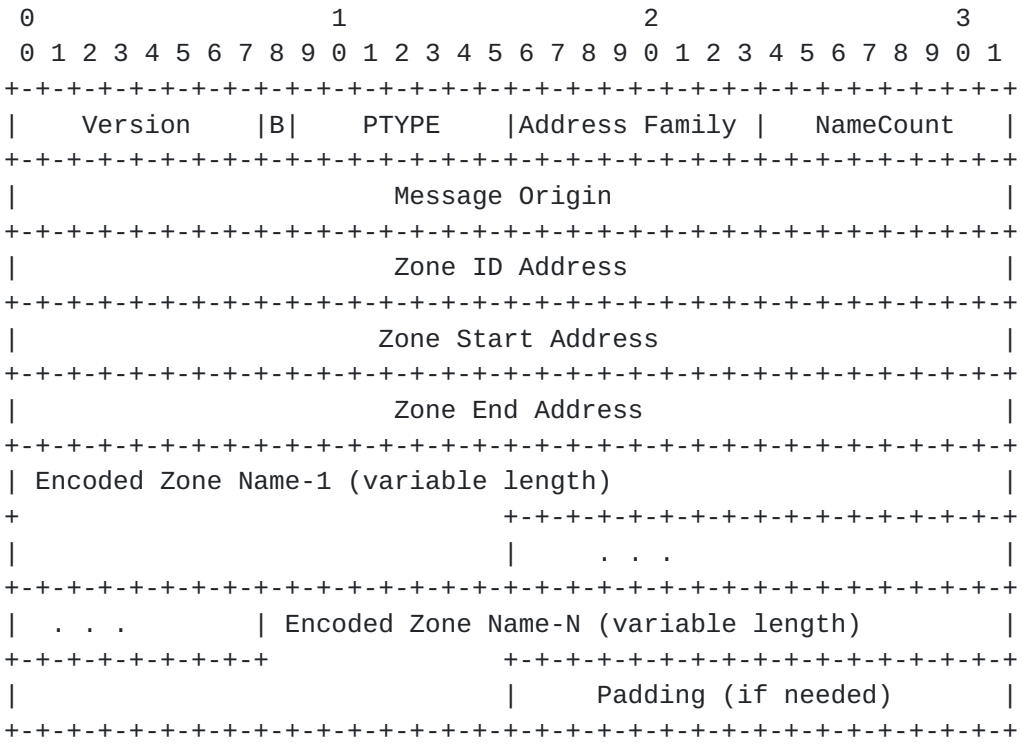
- If a ZBR is configured with a non-empty scope name for a given scope, and it receives a ZAM with a non-empty scope name for the same scope, and the scope names do not match.

Detecting either type of conflict above indicates that either the local router or router originating the message is misconfigured.
Configuration tools SHOULD strip white space from the beginning and end

of each name to avoid accidental misconfiguration.

3.7. Packet Formats

All MZAP messages are sent over UDP, with a destination port of [MZAP-PORT]. The common MZAP message header (which follows the UDP header), is shown below:



Version:
The version defined in this document is version 0.

"Big" scope bit (B):
If clear, indicates that the addresses in the scoped range are not subdividable, and that address allocators may utilize the entire range. If set, address allocators should not use the entire range, but should learn an appropriate sub-range via another mechanism (e.g., AAP [7]).

Packet Type (PTYPE):
The packet types defined in this document are:
0: Zone Announcement Message (ZAM)
1: Zone Limit Exceeded (ZLE)
2: Zone Convexity Message (ZCM)
3: Not-Inside Message (NIM)

Address Family:
The IANA-assigned address family number identifying the address family for all addresses in the packet. The families defined for IP are:
1: IPv4
2: IPv6

Name Count:
The number of encoded zone name blocks in this packet. The count may be zero.

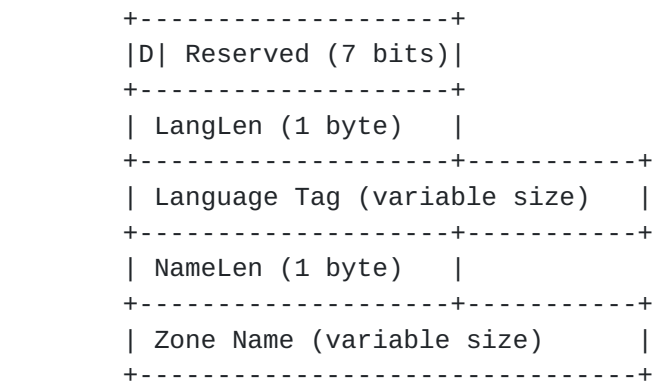
Zone Start Address: 32 bits (IPv4) or 128 bits (IPv6)
This gives the start address for the scope zone border. For example, if the zone is a border for 239.1.0.0 to 239.1.0.255, then Zone Start Address is 239.1.0.0.

Zone End Address: 32 bits (IPv4) or 128 bits (IPv6)
This gives the ending address for the scope zone border. For example, if the zone is a border for 239.1.0.0 to 239.1.0.255, then Zone End Address is 239.1.0.255.

Message Origin: 32 bits (IPv4) or 128 bits (IPv6)
This gives the IP address of the interface that originated the message.

Zone ID Address: 32 bits (IPv4) or 128 bits (IPv6)
This gives the lowest IP address of a boundary router that has been observed in the zone originating the message. Together with Zone Start Address and Zone End Address, it forms a unique ID for the zone. Note that this ID is NOT the ID of the Local Scope zone in which the origin resides.

Encoded Zone Name:



The first byte contains flags, of which only the high bit is defined. The other bits are reserved (sent as 0, ignored on receipt).

"Default Language" (D) bit:
If set, indicates a preference that the name in the following language should be used if no name is available in a desired language.

Language tag length (LangLen): 1 byte
The length, in bytes, of the language tag.

Language Tag: (variable size)
The language tag, such as "en-US", indicating the language of the zone name. Language tags are described in [6].

Name Len:
The length, in bytes, of the Zone Name field. The length MUST NOT be zero.

Zone Name: multiple of 8 bits
The Zone Name is an ISO 10646 character string in UTF-8 encoding [4] indicating the name given to the scope zone (eg: ``ISI-West Site''). It should be relatively short and MUST be less than 256 bytes in length. White space SHOULD be stripped from the beginning and end of each name before encoding, to avoid accidental conflicts. All the border routers to the same region SHOULD be configured to give the same Zone Name, or a zero length string MAY be given. A zero length string is taken to mean that another router is expected to be configured with the zone name. Having ALL the ZBRs for a scope zone announce zero length names should be considered an error.

Padding (if needed):
The end of the MZAP header is padded with null bytes until it is 4-

byte aligned.

3.7.1. Zone Announcement Message

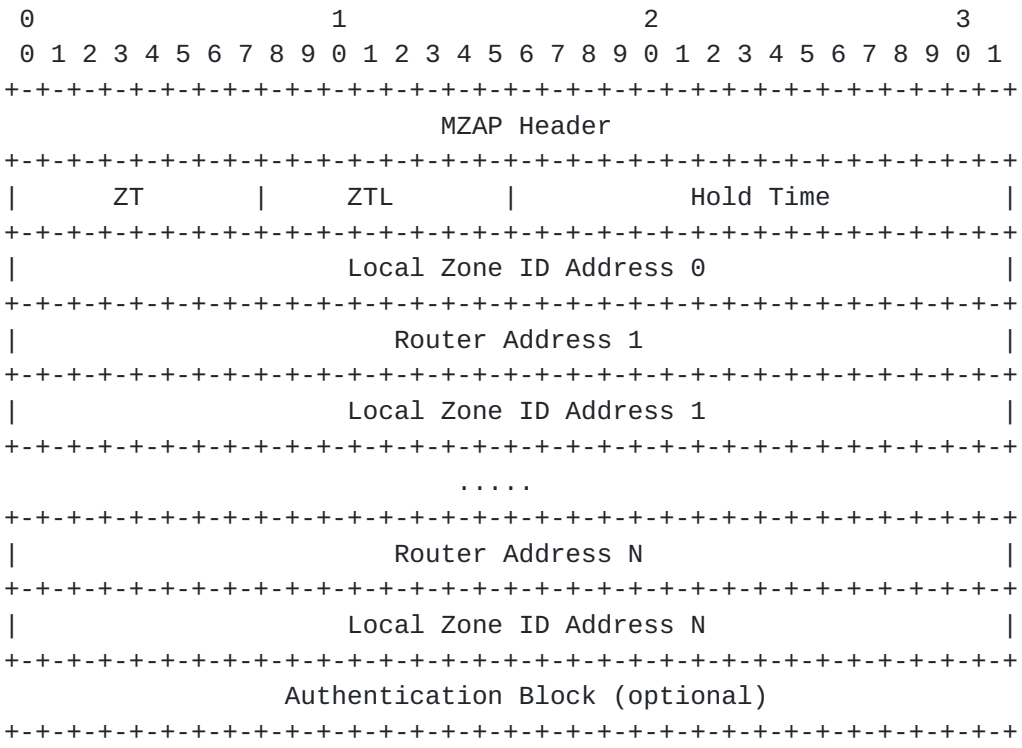
A Zone Announcement Message has PTYPE=0, and is periodically sent by a ZBR for each scope for which it is a border, EXCEPT:

o the Global Scope

o the Local Scope

o the Link-local scope

The format of a Zone Announcement Message is shown below:



The fields are defined as follows:

Zones Traveled (ZT): 8 bits
This gives the number of Local Zone IDs contained in this message path.

Zones Traveled Limit (ZTL): 8 bits
This gives the limit on number of local zones that the packet can traverse before it MUST be dropped. A value of 0 indicates that no limit exists.

Hold Time:
The time, in seconds, after which the receiver may assume the scope no longer exists, if no subsequent ZAM is received. This should be set to [ZAM-HOLDTIME].

Zone Path: multiple of 64 bits (IPv4) or 256 bits (IPv6)
The zone path is a list of Local Zone ID Addresses (the Zone ID Address of a local zone) through which the ZAM has passed, and IP addresses of the router that forwarded the packet. The origin router fills in the "Local Zone ID Address 0" field when sending the ZAM. Every Local Scope router that forwards the ZAM across a Local Scope boundary MUST add the Local Zone ID Address of the local zone that the packet of the zone into which the message is being forwarded, and its own IP address to the end of this list, and increment ZT accordingly. The zone path is empty which the ZAM is first sent.

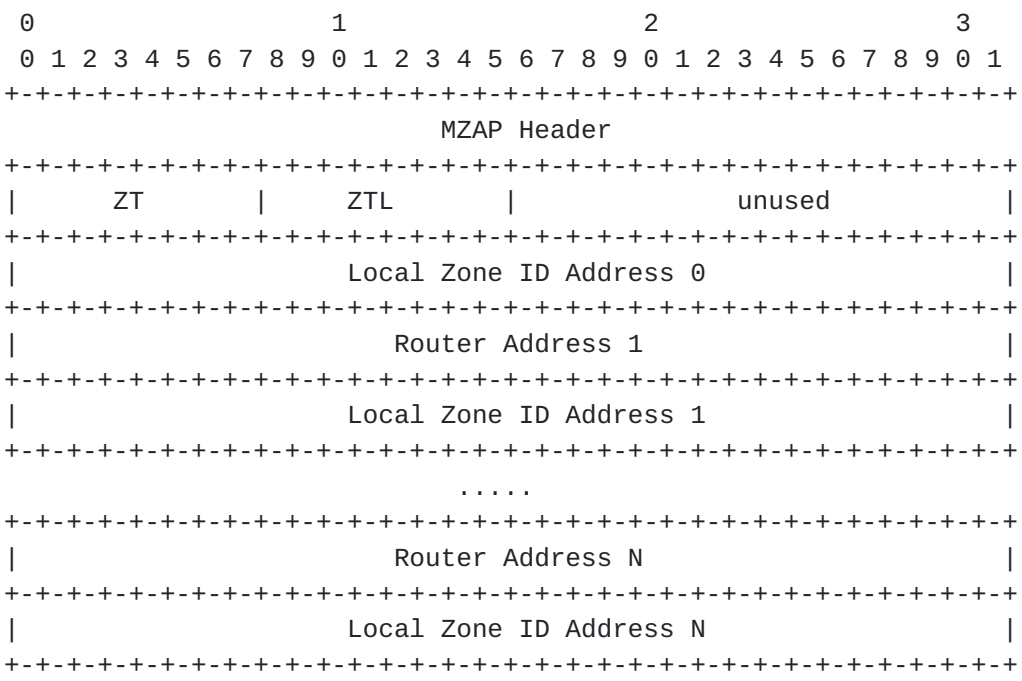
Authentication Block:
If present, this provides information which can be used to authenticate the sender of the ZAM (i.e. Router Address N, if ZT is non-zero, or Message Origin, if ZT is zero). (TBD: any reason not to re-use SAP's "Authentication Header" here?)

3.7.2. Zone Limit Exceeded (ZLE)

This packet is sent by a local-zone border router that would have exceeded the Zone Traveled Limit if it had forwarded a ZAM packet. To avoid ZLE implosion, ZLEs are multicast with a random delay and suppressed by other ZLEs. It is only scheduled if at least [ZLE-MIN-INTERVAL] seconds have elapsed since it previously sent a ZLE to any destination. To schedule a ZLE, the router sets a random delay timer within the interval [ZLE-SUPPRESSION-INTERVAL], and listens to the [MZAP-RELATIVE-GROUP] within the included scope for other ZLEs. If any are received before the random delay timer expires, the timer is cleared and the ZLE is not sent. If the timer expires, the router sends a ZLE to the [MZAP-RELATIVE-GROUP] within the indicated scope.

The method used to choose a random delay (T) is as follows:
Choose a random value X from the uniform random interval [0:1]
Let C = 256
Set T = [ZLE-SUPPRESSION-INTERVAL] log(C*X + 1) / log(C)
This method ensures that close to one ZBR will respond.

The format of a ZLE is shown below:



All fields are copied from the ZAM, except PTYPE which is set to one.

A router receiving ZLE messages SHOULD log them and attempt to alert the network administrator that the scope zone is misconfigured.

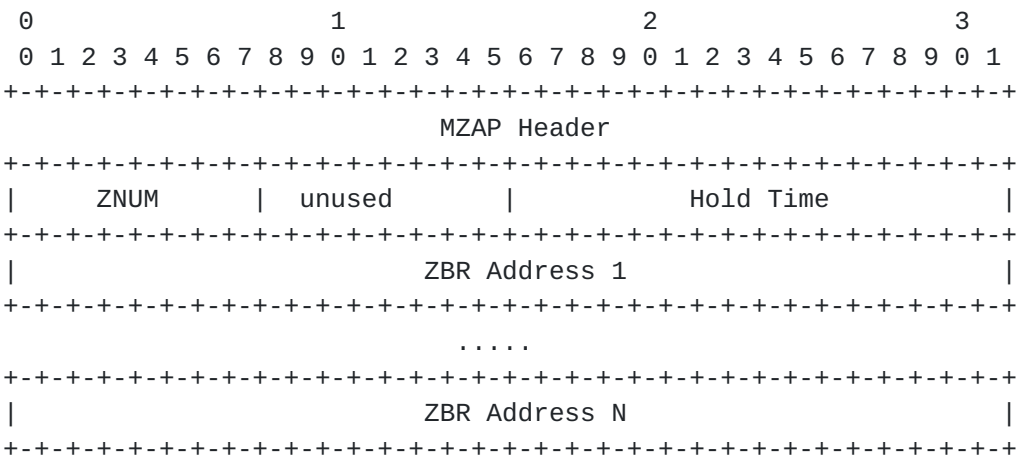
3.7.3. Zone Convexity Message

A Zone Announcement Message has PTYPE=2, and is periodically sent by a ZBR for each scope for which it is a border, EXCEPT:

o the Global Scope

o the Link-local scope
(Note that ZCM's ARE sent in the Local Scope.)

Unlike Zone Announcement Messages which are sent to the [MZAP-LOCAL-GROUP], Zone Convexity Messages are sent to the [ZCM-RELATIVE-GROUP] in the scope zone itself. The format of a ZCM is shown below:



The fields are as follows:

Number of ZBR addresses (ZNUM): 8 bits

This field gives the number of ZBR Addresses contained in this message.

Hold Time:

The time, in seconds, after which the receiver may assume the sender is no longer reachable, if no subsequent ZCM is received. This should be set to [ZCM-HOLDTIME].

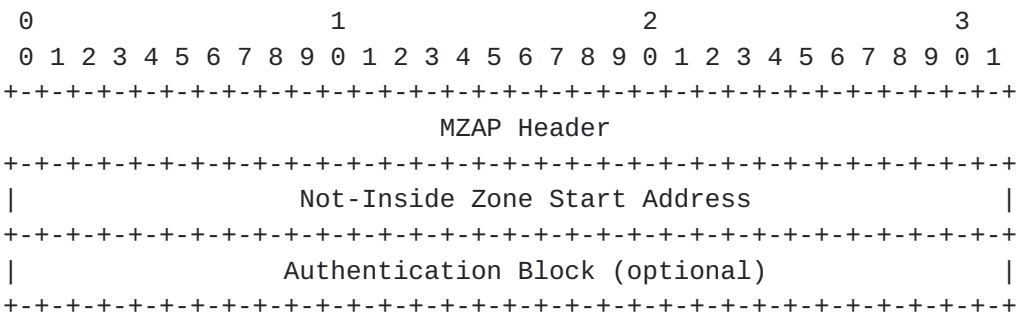
ZBR Address: 32 bits (IPv4) or 128 bits (IPv6)

These fields give the addresses of the other ZBRs from which the Message Origin ZBR has received ZCMs but whose hold time has not expired. The router should include all such addresses which fit in the packet, preferring those which it has not included recently if all do not fit.

3.7.4. Not-Inside Message

A Not-Inside Message (NIM) has PTYPE=3, and is periodically sent by a ZBR which knows that a scope X does not nest within another scope Y ("X not inside Y"):

The format of a Not Inside Message is shown below:



The fields are as follows:
MZAP Header:
   Header fields identifying the scope X. The Name Count may be 0.

Not-Inside Zone Start Address: 32 bits (IPv4) or 128 bits (IPv6)
   This gives the start address for the scope Y.

Authentication Block:
   If present, this provides information which can be used to authenticate the sender of the NIM (i.e. Message Origin in the MZAP Header).

4. Message Timing

Each ZBR should send a Zone Announcement Message for each scope zone for which it is a boundary every [ZAM-INTERVAL] seconds, +/- 30% of [ZAM-INTERVAL] each time to avoid message synchronisation.

Each ZBR should send a Zone Convexity Message for each scope zone for which it is a boundary every [ZCM-INTERVAL] seconds, +/- 30% of [ZCM-INTERVAL] each time to avoid message synchronisation.

A router SHOULD NOT send more than one Zone Limit Exceeded message every [ZLE-MIN-INTERVAL] regardless of destination.

Each ZBR should send a Zone State Session Message for each scope zone for which it is a boundary every [ZNSM-INTERVAL] seconds, +/- 30% of [ZNSM- INTERVAL] each time to avoid message synchronization.

5. Constants

[MZAP-PORT]: The well-known UDP port to which all MZAP messages are sent. Value: TBD by IANA.

[MZAP-LOCAL-GROUP]: The well-known group in the Local Scope to which ZAMs are sent. All Multicast Address Allocation servers and Zone Border Routers listen to this group. Value: TBD by IANA.

[ZCM-RELATIVE-GROUP]: The relative group in each scope zone, to which ZCMs are sent. A Zone Border Router listens to the relative group in each scope for which it is a border. Value: TBD by IANA.

[ZAM-INTERVAL]: The interval at which a Zone Border Router originates Zone Announcement Messages. Default value: 600 seconds (10 minutes).

[ZAM-HOLDTIME]: The holdtime to include in a ZAM. This SHOULD be set to at least 3 * [ZAM-INTERVAL]. Default value: 1860 seconds (31 minutes).

[ZAM-DUP-TIME]: The time interval after forwarding a ZAM, during which ZAMs for the same scope will not be forwarded. Default value: 30 seconds.

[ZCM-INTERVAL]: The interval at which a Zone Border Router originates Zone Convexity Messages. Default value: 600 seconds (10 minutes).

[ZCM-HOLDTIME]: The holdtime to include in a ZCM. This SHOULD be set to at least 3 * [ZCM-INTERVAL]. Default value: 1860 seconds (31 minutes).

[ZLE-SUPPRESSION-INTERVAL]: The interval over which to choose a random delay before sending a ZLE message. Default value: 300 seconds (5 minutes).

[ZLE-MIN-INTERVAL]: The minimum interval between sending ZLE messages, regardless of destination. Default value: 300 seconds (5 minutes).

[NIM-INTERVAL]: The interval at which a Zone Border Router originates Zone Not Inside Messages. Default value is 1800 seconds (30 minutes)

[NIM-HOLDTIME]: The holdtime to include the state within a NIM. This SHOULD be set to at least 3 * [NIM-INTERVAL]. Default value: 5460 (91 minutes)

6. Security Considerations

MZAP does not include authentication in its messages. Thus it is open to misbehaving hosts sending spoof ZAMs, ZCMs, or NIMs.

In the case of ZCMs, these spoof messages can cause false logging of convexity problems. It is likely that is would be purely an annoyance, and not cause any significant problem.

In the case of ZAMs, spoof messages can also cause false logging of configuration problems. This is also considered to not be a significant problem.

In the case of NIMs, spoof messages can also cause the false cancellation of nesting relationships. This would cause a section of the hierarchy of zones to flatten. Such a flattening would lessen the efficiency benefits afforded by the hierarchy but would not cause it to become unusable.

Spoofed zone announcements however might cause applications to believe that a scope zone exists when it does not. If these were believed, then applications may choose to use this non-existent administrative scope zone for their uses. Such applications would be able to communicate successfully, but would be unaware that their traffic may be traveling further than they expected. As a result, applications MUST only take scope names as a guideline, and SHOULD assume that their traffic sent to non-local scope zones might travel anywhere. The confidentiality of such traffic CANNOT be assumed from the fact that it was sent to a scoped address that was discovered using MZAP.

In addition, ZAMs are used to inform Multicast Address Allocation Servers of names of scopes, and spoofed ZAMs would result in false names being presented to users. To counter this, ZAMs may be authenticated as follows:

(1) A ZBR signs all ZAMs it originates.

(2) A ZBR signs a ZAM it forwards if and only if it can authenticate the previous sender. A ZBR MUST still forward un-authenticated ZAMs (to provide leak detection), but should propagate an authenticated ZAM even if an un-authenticated one was received with the last [ZAM-DUP-TIME] seconds.

(3) A MAAS SHOULD be configured with the public key of the local zone in which it resides. A MAAS thus configured SHOULD ignore an unauthenticated ZAM if an authenticated one for the same scope has been received, and MAY ignore all unauthenticated ZAMs.

7. References

[1] Meyer, D., "Administratively Scoped IP Multicast", RFC 2365, July 1998.

[2] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997.

[3] Handley, M., Thaler, D., and D. Estrin, "The Internet Multicast Address Allocation Architecture", Internet Draft, Dec 1997.

[4] Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, January 1998.

[5] Fenner, W., and S. Casner, "A ''traceroute'' facility for IP Multicast", draft-ietf-idmr-traceroute-ipm-02.txt, Internet Draft, November 1997.

[6] Alvestrand, H., "Tags for the Identification of Languages", RFC 1766, March 1995.

[7] Handley, M., "Multicast Address Allocation Protocol (AAP)", draft-handley-aap-01.txt, Internet Draft, July 1998.

[8] Kermode, R. "Scoped Hybrid Automatic Repeat reQuest with Forward Error Correction (SHARQFEC)", ACM SIGCOMM 98, September 1998, Vancouver, Canada.

8. Acknowledgements

This document is a product of the MBone Deployment Working Group, whose members provided many helpful comments and suggestions. The Multicast Address Allocation Working Group also provided useful feedback regarding scope names and interactions with applications.

9. Authors' Addresses

Mark Handley
AT&T Center for Internet Research at ICSI
1947 Center St, Suite 600
Berkely, CA 94704
USA
Email: mjh@aciri.org

David Thaler
Microsoft
One Microsoft Way
Redmond, WA 98052
USA
Email: dthaler@microsoft.com

Roger Kermode
Motorola Australian Research Centre
12 Lord St,
Botany, NSW 2109
Australia
Email: Roger_Kermode@email.mot.com

10. Full Copyright Statement

Table of Contents