Internet Engineering Task Force
INTERNET-DRAFT
draft-draft-handley-aap-00.ps

MALLOC WG
M. Handley
ISI

December 15, 1997
Expires: June 1998

Multicast Address Alloctation Protocol (AAP)

Status of this Memo

Abstract

The document defines a Multicast Address Allocation Protocol (AAP) that forms a part of a larger multicast address allocation architecture currently being defined. AAP addresses the specific issue of intra-domain multicast address allocation between multicast address allocation servers.

1 Introduction

This document defines a Multicast Address Allocation Protocol (AAP) that forms a part of a larger multicast address allocation architecture[1]. The general framework with which AAP is designed to operate is best describes by describing the process by which a multicast address is allocated:

1. As a continuous process, a higher level protocol, MASC [2], provides a multicast address set to an allocation domain that multicast addresses should be allocated out of.

2. MASC routers periodically send advertisements of this address set to Multcast Address Allocation Servers (MAAS) within the allocation domain using AAP address-set advertisement messages.

3. When a client requires a multicast address, it sends a request to a MAAS server for information about the scope zones that include the server. The MAAS server returns this information.

4. The client then chooses a scope zone, and requests an address for a certain period of time.

5. The MAAS server chooses an address from the address set that is not currently in use, and multicasts an AAP prospective-announcement message to all the other MAAS servers in the allocation domain. If no-one objects to this announcement, then the MAAS server starts to periodically multicast an AAP address-in-use message to all the MAAS servers in the allocation domain, and it returns the address to the client to use.

1.1 Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [10] and indicate requirement levels for compliant SIP implementations.

1.2 Definitions

2 Specification of Behaviour

Within an allocation domain, MAAS servers are all multicast peers - there is no hierarchy or configured peering. To allocate an address, a MAAS server should have been listening to AAP address-set messages and AAP address-in-use messages for a considerable period of time (known at STARTUP-WAIT) so that it has a good idea of currently available addresses. MAAS servers that have not been listening for at least STARTUP-WAIT SHOULD NOT respond to a client's request for an address.

2.1 AAP Packet Types

The following packet types are defined:

ADDRESS-SET-ANNOUNCE

This AAP message is sent from a MASC router to all the MAAS servers in an allocation domain. It lists a number of address-sets, each of which has an associated lifetime. The announcement contains a timestamp to detect replays or broken clocks, a refresh time, and the address of the last MASC router to send an ADDRESS-SET-ANNOUNCE message to this group.

The address-set contained in such a message MUST be the complete address-set available to MAAS servers at that time. An address-set MUST NOT be spilt across multiple ADDRESS-SET-ANNOUNCE messages.

The expiry time is the time by which all MAAS servers within the domain should reasonably have heard a new ADDRESS-SET-ANNOUNCE message. If no ADDRESS-SET-ANNOUNCE message is forthcoming by this expiry time, this MAY be used to raise alarms that some unexpected failure has occured. Addresses SHOULD still be allocated by such a MAAS server, but request protocols that permit it MAY report a lack of confidence in the address.

ADDRESS-SET-ANNOUNCE messages MAY alternate between several cooperating MASC routers. Each ADDRESS-SET-ANNOUNCE message contains the address of the last router to send such a message to the domain. This information is present to detect cases where two MASC routers are sending messages to the domain without hearing each others messages. It may not be counted upon for any other purpose.

ADDRESS-SET-ANNOUNCE messages MUST be digitally signed by the router that sends them. MAAS servers MAY be configured to ignore ADDRESS-SET-ANNOUNCE messages from unknown routers.

SERVER-SIGNATURE

This AAP message gives the public key of a new server and the expiry time for this key. Such a server can be a new MAAS server or a new MASC router. This key MUST be digitally signed by one or more additional servers. It may be multicast from any node in the allocation domain to all the MAAS servers in the domain, and is used to bootstrap the trust of both MASC routers and MAAS servers.

PROVISIONAL-ADDRESS-ALLOCATION

This AAP message is multicast from a MAAS server attempting to allocate an address to all other MAAS servers in the domain. The message contains a list of the addresses being requested, the beginning and end times for the allocation, and a request sequence number.

The MAAS server sending this message has already listened to other announcements, and is reasonably certain that the addresses listed are not in use. It sends this message to check that it has not missed a recent announcement by another MAAS server. It expects that no reply will be forthcoming, but waits ANNOUNCE-WAIT seconds to ensure this is the case.

Two possible messages might be received that would indicate a problem with the announcement.

- ADDRESS-SET-ANNOUNCE might be sent by a MASC router to indicate that the address allocation was not valid for the address-set currently available. This is extremely unlikely to occur with a compliant MAAS server, and MASC routers are not required to listen to AAP PROVISIONAL-ADDRESS-ALLOCATION messages.
- ADDRESS-IN-USE might be sent be another MAAS server to indicate that the address was already in use. This can be sent if the same address is already allocated for the same time interval.

In either case, the MAAS server SHOULD change its allocation and send another PROVISIONAL-ADDRESS-ALLOCATION message with the same request sequence number. The only exception to this is if the MAAS server suspects a denial of service attack is in progress (see section 5.1).

This message MAY be digitally signed by the MAAS server sending it.

ADDRESS-IN-USE

This AAP message is multicast periodically from a MAAS server to all other MAAS servers in the domain to indicate that addresses are in use. The message contains a list of addresses, each with an associated start and stop time.

This message may also be sent by any MAAS server that notices a PROVISIONAL-ADDRESS-ALLOCATION message that would cause a clash. See section XXX for details of the timing of such response messages.

This message MAY be digitally signed by the MAAS server sending it.

ADDRESS-DELETION

This AAP message is multicast once by the same MAAS server that listed the address contained in the message in an ADDRESS-IN-USE message. It is OPTIONAL. If it is sent, it MUST be digitally signed. It MUST NOT be sent unless the corresponding ADDRESS-IN-USE message was also digitally signed.

ADDRESS-SPACE-REQUIRED

The AAP message is periodically multicast from a MAAS server to all the MASC routers for the domain indicating the current address space requirements. It contains a set of numbers of addresses and the expiry dates for each of those numbers of addresses.

These messages SHOULD be digitally signed. If any MAAS server in the domain is trusted by the MASC routers, that server should send the ADDRESS-SPACE-REQUIRED messages. If not, any MAAS server may take over this role. This is achieved by using shorter randomised timeouts for the trusted servers as explained in section XXX. How the MAAS server calculates the address space required is explained in section XXX.

.

3 Specification of MAAS Server Behaviour

When a MAAS server starts up, it MUST listen to AAP messages for at least START-WAIT time before it can respond to an address allocation request, and SHOULD have received at least one ADDRESS-SET-ANNOUNCE message. If it does not receive an ADDRESS-SET-ANNOUNCE message within this time, it MAY respond to an allocation request only if it has cached a previous ADDRESS-SET-ANNOUNCE message which includes at least one range that has not reached its end time.

When a MAAS server receives a request for the allocation of an address, that request will contain a start and end-time. The MAAS server SHOULD choose the address-set from those that were advertised to it that satisfies the greatest proportion of the time in the request. From that address-set it SHOULD then choose at random an address that is not already being advertised by any MAAS server. It should then send this address in a PROVISIONAL-ADDRESS-ALLOCATION message with the start-time from the request and the minimum of the address-set end-time and the request end-time. It SHOULD then set a timer for ANNOUNCE-WAIT seconds in the future.

If the MAAS server receives a PROVISIONAL-ADDRESS-ALLOCATION message or an ADDRESS-IN-USE message from another MAAS server listing the same addres before the timer expires, then it should cancel the timer, choose another address in the same manner, send another PROVISIONAL-ADDRESS-ALLOCATION message listing the new address, and set a new timer for ANNOUNCE-WAIT seconds in the future. Such a MAAS server MAY also resend the PROVISIONAL-ADDRESS-ALLOCATION after RESEND-WAIT seconds, and again after a further RESEND-WAIT*2 seconds, doubling each time until the timer expires.

If the timer expires, the MAAS server can conclude that there is a good probability that the address is unique, and it can then send an ADDRESS-IN-USE message listing this address, add the address to its list of allocated addresses, and return the address along with the (possibly modified) end-time to the client.

A MAAS server MUST send ADDRESS-IN-USE messages periodically for all the addresses that it currently has allocated. Each of these addresses SHOULD be included in an ADDRESS-IN-USE message every BASE-REPEAT-INTERVAL seconds +/- 30% of this value to avoid synchronisation effects. A MAAS server that has allocated an address MAY resend that address again after RESEND-WAIT seconds, and again after a further RESEND-WAIT*2 seconds, doubling each time until the interval reached BASE-REPEAT-INTERVAL seconds.

In some circumstances a MAAS server may receive large numbers of requests for addresses, each for very short period of time. Sending triggered announcements for each of these requests increases the delay before granting addresses and may create a significant amount of AAP traffic. If it desires, such a server MAY pro-actively allocate a pool of addresses using the process described above, and may then may grant these requests immediately out of this pool. As the server MUST have already sent ADDRESS-IN-USE messages for these pooled addresses, there should be no clash. Such servers should maintain the minimum pool to allow them to perform their task well. Applications requiring multicast addresses MUST NOT assume that a MAAS server will always grant them addresses with no delay, and SHOULD assume that the server will take at least ANNOUNCE-WAIT seconds to allocate them an address. Depending on the request protocol being used by the client, a server MAY communicate ANNOUNCE-WAIT to clients when they request a list of current scope zones before requesting a multicast address, or it MAY send an interrim reply to the client indicating how long it expects allocation to take.

3.1 Triggered Responses

When a MAAS server A receives a PROVISIONAL-ADDRESS-ALLOCATION message from MAAS server B containing an address that clashes with an address in its cache, it should set a timer based on the algorithm below. If server A sees an ADDRESS-IN-USE message from a server other than B containing this address before the timer expires, it should restart the timer with double its original value. If server A sees a PROVISIONAL-ADDRESS-ALLOCATION from server B with the same sequence number as before, it should cancel its timer.

If server A's timer expires, it should send an ADDRESS-IN-USE message containing the address in question, and should restart the timer with twice its previous value, unless that value was 0, in which case it sets it to INITIAL-TIMER.

The initial value for the timer is determined as follows:

- If server A is the server that was originating the announcement for the address in question, the initial value of the timer is 0.
- If server A is not the server that was originating the announcement for this address, the server calculates the timer, t, as follows:

  X is chosen from the uniform random interval [0:1]

  $t = D_1 + R * log_2((2^{(D_2/R)} * X + 1)$

  D_1 defaults to R.
  D_2 defaults to DEFAULT-D2 seconds.

  R is an estimate of maximum round trip time for the domain, and defaults to DEFAULT-RTT. This value MAY be reduced to reduce delays for some domains. If the value is increased, it MUST be increased in all MAAS servers in the domain.

  This equation results is an exponential random distribution between D_1 and D_2 seconds. The value of D_2 is useful for up to several thousand MAAS servers in a domain to ensure that close to one server responds.

If a MAAS server has sent a PROVISIONAL-ADDRESS-ALLOCATION message and has an ANNOUNCE-WAIT timer running, and it receives another PROVISIONAL-ADDRESS-ALLOCATION message from another MAAS server, it SHOULD immediately choose another multicast address and send a new PROVISIONAL-ADDRESS-ALLOCATION message with the same sequence number. It MUST NOT send an ADDRESS-IN-USE message in this state in response to a PROVISIONAL-ADDRESS-ALLOCATION message. It does not matter which server chooses a new address in these circumstanes, so it is not necessary to inform the other site.

3.2 Scope of AAP Messages

AAP messages are sent to a well known multicast address (239.??.??.??) and port (????). This multicast address MUST be administratively scoped so as not to leave the allocation domain. The TTL on packets SHOULD be set to 255.

Note: AAP is not intended to perform multicast address allocation for TTL-scoped sessions. Non-global sessions SHOULD be constrained using administrative scoping only.

3.3 AAP Timers

The following AAP timers are defined:

START-WAIT

START-WAIT = Max(5 * SET-REPEAT-INTERVAL, 5 * BASE-REPEAT-INTERVAL) seconds.

SET-REPEAT-INTERVAL

SET-REPEAT-INTERVAL defaults to 30 seconds.

ANNOUNCE-WAIT

ANNOUNCE-WAIT defaults to 3 seconds.

RESEND-WAIT

RESEND-WAIT defaults to 1 second.

INITIAL-TIMER

INITITAL-TIMER defaults to DEFAULT-RTT.

DEFAULT-RTT

DEFAULT-RTT defaults to 100ms.

DEFAULT-D2

DEFAULT-D2 defaults to 3.0s.

BASE-REPEAT-INTERVAL

BASE-REPEAT-INTERVAL = Max(30, SIZE*NO-OF-ADDRESSES/BASE-RATE) seconds.

where:

NO-OF-ADDRESSES is the number of addresses currently allocated within the domain.

SIZE is the size in bytes of a single (address,start-time,stop-time) triple from an ADDRESS-IN-USE message.

BASE-RATE

BASE-RATE is the approximate background rate for announcement traffic within a domain with a significant number of addresses allocated. For IPv4, the rate only reaches this level with around 3000 addresses allocated within a domain.

It defaults to 1250 bytes/second.

4 Packet Formats

AAP messages are binary format, as the additional flexibility of having a textual format is not required in this case.

All AAP packets start with the following common header:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  V=0  |STYPE|P|       SLEN      | PTYPE | ATYPE |       SEQ       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

version (V): 4 bits

This field identified the version of AAP. The version defined by this specification is 0.

Signature Type (STYPE): 4 bits

This field identifies the type of digital signature used to sign the message. The values are defined as follows:

0. No signature present. SLEN MUST also be zero.
1. PGP signature used. The format is described in TBD.

Signature Length (SLEN): 8 bits

This field indicates the length of the digital signature in the packet as a multiple of 32 bit words. If the signature is not a multiple of 32 bits long, the last byte of the signature indicates the number of padding bytes that have been added to the end of the signature. These padding bytes are then included in the signature length, and the signature padding bit (P) is set.

Packet Type (PTYPE): 4 bits

This field indicates the type of AAP packet this is. It is one of the following values:

0. ADDRESS-SET-ANNOUNCE
1. SERVER-SIGNATURE
2. PROVISIONAL-ADDRESS-ALLOCATION
3. ADDRESS-IN-USE
4. ADDRESS-DELETION
5. ADDRESS-SPACE-REQUIRED

Address Type (ATYPE): 4 bits

This field indicates the address type used in the packet. Multiple address types (for example IPv4 and IPv6) can be used within the same domain at the same time. However, only a single address type may be used within one AAP packet.

The following values are defined:

0. IP version 4.

1. IP version 6.

Sequence (SEQ): 8 bits

This field is a sequence number. The first packet an AAP host sends should have sequence number 0, and the sequence number should be incremented for every subsequent packet, modulo 256.

The sequence number is not needed to uniquely identify packets, but can be used to get an idea of packet loss rates within an allocation domain. This information may be useful in deciding some parameters for address allocation.

Immediately following the common header is a digital signature of the payload of the packet. This can be of variable length.

Following the digital signature are the packet contents, the format of which depend on both the ATYPE and PTYPE fields.

4.1 AAP Time Fields

AAP packets contain a number of places where absolute times must be represented. Unless otherwise stated, these time values are represented as unsigned 32 bit integers in network byte order giving the number of seconds since 00:00 UTC, 1st January 1970. This arbitrary baseline is convenient on many current operating systems, and can be converted to an NTP timestamp by adding decimal 2208988800. Thus AAP time fields will not wrap until the year 2106.

4.2 IPv4 Packet Formats (ATYPE=0)

4.2.1 ADDRESS-SET-ANNOUNCE

An address set announce packet for IPv4 contains an address set refresh time, followed by one or more address sets:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Current Time                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Refresh Time                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Multicast Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              Mask                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Expiry time                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Multicast Address                     |
|/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/|
```

The current time is an AAP time field (see section 4.1) and gives the current time at the router sending this message.

The address set refresh time is an AAP time field giving the time by which another ADDRESS-SET-ANNOUNCE message should have been received.

Within each address set, the multicast address indicates an IPv4 base address. The mask indicates which bits from the base address are wildcarded, i.e, can be set be the address allocater. For example, if the base address is: 0xE0020000 (224.2.0.0) and the mask is 0x000100FF then addresses 224.2.0.0-224.2.0.255 and 224.3.0.0-224.3.0.255 are available. Note that the mask does not have to be contiguous. All MAAS servers MUST be able to cope with discontiguous masks, although in some cases only contiguous masks may be supplied by MASC.

The address set expiry time is an AAP time field giving the time at which the address set will expire. Addresses should only be granted from this address set up until this time.

4.2.2 SERVER-SIGNATURE

TBD

4.2.3 PROVISIONAL-ADDRESS-ALLOCATION

A PROVISIONAL-ADDRESS-ALLOCATION packet for IPv4 contains the current time at the MAAS server and one or more addresses:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Current Time                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Multicast Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Start time                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           End time                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Multicast Address                     |
|/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/|
```

The multicast address lists the specific address being requested. Start-time and end-time are AAP time fields giving the range of time for which the address is required.

Multicast addresses within the packet MUST be in increasing numerical order.

4.2.4 ADDRESS-IN-USE

An ADDRESS-IN-USE packet for IPv4 contains the current time at the MAAS server, a refresh timeout, and one or more addresses as for PROVISIONAL-ADDRESS-ALLOCATION.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Current Time                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Refresh Time                         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Multicast Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Start time                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           End time                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Multicast Address                     |
|/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/|
```

The current-time is an AAP time field used to discover MAAS servers that have incorrectly set clocks, or to identify the age of proxy announcements when a MAAS server has died.

Multicast addresses within the packet MUST be in increasing numerical order. Where a MAAS server has more addresses than will fit in one packet, they may be split over several packets. There SHOULD be no overlap in numerical ranges of addresses between these packets. An exception to this is if a MAAS server is announcing its own addresses and those of another server, when it SHOULD announce its own addresses in different packets from those it is proxy announcing. Ordering the addresses in this way increases the efficiency of processing packets received at a MAAS server.

The refresh-time is an AAP time field used to indicate that another message from the same server should have been received by this time. This time SHOULD be far enough in the future that at least five messages from this server would have been expected to have been heard. If no messages are heard in this interval, other MAAS servers MAY conclude that this MAAS server has died or been partitioned. In such circumstances they MAY make a proxy announcement (see section XXX).

4.2.5 ADDRESS-DELETION

An ADDRESS-DELETION packet for IPv4 contains one or more addresses:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    IPv4 Multicast Address                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

4.2.6 ADDRESS-SPACE-REQUIRED

An ADDRESS-SPACE-REQUIRED packet for IPv4 contains one or more pairs of number of addresses and lifetimes:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      number of addresses                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          end-time                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Generally speaking, if the MAAS server is happy with its current address set, it should simply report the address set back to the MASC servers with this message.

However, if the address space is insufficient, the MAAS server should either add one of more additional pairs of number of addresses and lifetime, or increase the number of addresses from one of the existing pairs.

If the address set is larger than required, this is not usually dealt with until addresses need to be allocated from a set with a longer lifetime than those in the existing set. At this time, the MAAS server will replace one or more of the pairs from the existing set with a smaller but longer duration pair.

Is this sufficient for suitable interaction between AAP and MASC? We could have the MAAS servers indicate which partitions they don't want to renew, which would entail a different ADDRESS-SPACE-REQUIRED packet format - MJH.

4.3 IPv6 Packet Formats (ATYPE=1)

TBD

5 Security

5.1 Denial of Service Attacks

TBD

References

[1] M. Handley, D. Thaler, D. Estrin, “The Internet Multicast Address Allocation Architecture”, Internet Draft, Dec 1997.

[2] D. Estrin, M, Handley, S. Kumar, D. Thaler, “The Multicast Address Set Claim (MASC) Protocol”, Internet Draft, Nov 1997.