Multicast Address Allocation Protocol (AAP).

Mark Handley, *USC/ISI*

AAP Requirements

The requirements for AAP are:

- For many servers within the same domain to be able to allocate addresses from a given address set.
- To achieve near 100% address space utilisation.
- To achieve low probability of address collision.
- To allocate addresses with a maximum delay of a few seconds.
- To use relatively little bandwidth.
- To be incrementally deployable.
- To be always available, and to be very resilient to network failures.

AAP Model

- **Within a domain there may be many MAAS servers allocating from the same address set.**
- **MAAS servers talk to each other using multicast AAP messages admin scoped to stay in the domain.**
- **All MAAS servers in a domain are peers**
  - There is no configured hierarchy, although there may be configured trust relationships.
- **MAAS servers announce to each other the addresses that are in use.**
  - Normally a MAAS server only announces the addresses it has allocated to its clients.

Allocating an Address (overview)

- **A MAAS server that wishes to allocate an address MUST have been listening for a fixed warm-up period to gather the current domain status.**
- **It chooses an address at random from those in the set that are not in use, and makes a PROVISIONAL-ADDRESS-ALLOCATION announcement to the AAP group.**
- **If no-one else responds, after a few seconds it starts making periodic ADDRESS-IN-USE announcements to the AAP group, and gives the address to its client.**
- **The ADDRESS-IN-USE announcements continue for the lifetime of the address.**

Allocating an Address: Collision supression

- **If a MAAS server hears a PROVISIONAL-ADDRESS-ALLOCATION for an address already in its cache, it can send an ADDRESS-IN-USE response even if it was not the MAAS server that allocated the address.**
- **To prevent response implosions, only the original allocator gets to respond immediately. Everyone else delays their response by a random amount, and is temporarily suppressed if they hear someone else respond.**
- **The suppression becomes permanent when the MAAS server that sent the PROVISIONAL-ADDRESS-ALLOCATION modifies the request.**

Pre-allocating Addresses

- **A MAAS server can pre-allocate addresses by allocating them before receiving a request.**
- **This is useful if the server gets many requests for short duration addresses and doesn't want to wait for responses during allocation, or to generate excessive triggered AAP traffic.**
- **As a rule, only busy servers should do this. Pre-allocated addresses should be marked as such to avoid confusing the mechanisms that need to ask for more addresses from MASC.**

Pre-choosing Addresses

- **This is similar to pre-allocation, but less assertive.**
- **A MAAS server can choose the next few addresses it will allocate, and announce this choice using AAP.**
- **This does NOT reserve the addresses, but it does warn other servers to avoid these addresses if possible, and hence reduces collision probability.**
- **The server MUST still send PROVISIONAL-ADDRESS-ALLOCATION messages as in a normal allocation when it actually wants to allocate the address.**
- **Pre-allocation and pre-choosing can both be used by the same server.**

Address Deletion

- **The primary mechanism to remove an address that has been allocated is for it to reach the end of its lifetime.**
- **If the ADDRESS-IN-USE messages announcing an address were digitally signed, addresses can be deleted by sending a digitally signed ADDRESS-DELETION message.**
- ***This is purely an optimisation.***
- **Many deletion messages may need to be sent before all MAAS servers have received the message and stopped proxy-announcing the address.**

Interaction with MASC routers

- **AAP is also used to convey address sets from MASC routers to MAAS servers, and to convey requests for more address space from MAAS servers to MASC routers.**
- **MASC routers periodically send ADDRESS-SET-ANNOUNCE messages to the AAP group.**
  - MAAS servers should only allocate out of this address set.
  - These messages MUST be digitally signed by the MASC router. MAAS servers may be configured to trust known routers in the event of conflicting address sets being distributed.

Interaction with MASC routers (2)

- **All MAAS servers send periodic ADDRESS-SPACE-REQUIRED messages reporting current or desired address space requirements.**
- **As they have access to the same data and use the same algorithm, they should be consistent.**
  - The messages can be digitally signed, and MASC routers can be configured to trust particular MAAS servers in the event of inconsistent reports being received.
  - MASC has a considerable amount of time to act on requests for more address space, so doesn't normally react to a single request, even from a trusted MAAS server.

Server Signatures

- **An additional AAP message type can be used to convey signed public keys for any MAAS server or MASc router.**
- **This is a bootstrap mechanism for server trust.**
- **A single MASC router can be configured to be trusted by MAAS servers. The trusted MASC router can then sign other MASC routers or MAAS servers' keys and distribute them this way, allowing those additional routers and servers to be trusted without needing additional prior knowledge of each other.**