Multicast and Unicast MAC Address Asignment Protocol (MUMAAP)

Antonio de la Oliva

InterDigital, UC3M

IEEE 802.1CQ Scope

- As defined in the PAR:

"This standard specifies protocols, procedures, and management objects for locally-unique assignment of 48-bit and 64-bit addresses to ports in IEEE 802 networks"

Actually, we are working on mechanisms for the distribution of Local MAC addresses (in the 802c defined SAI space) including stateful and stateless procedures, on a per-technology basis. This includes unicast and multicast local MAC addresses.

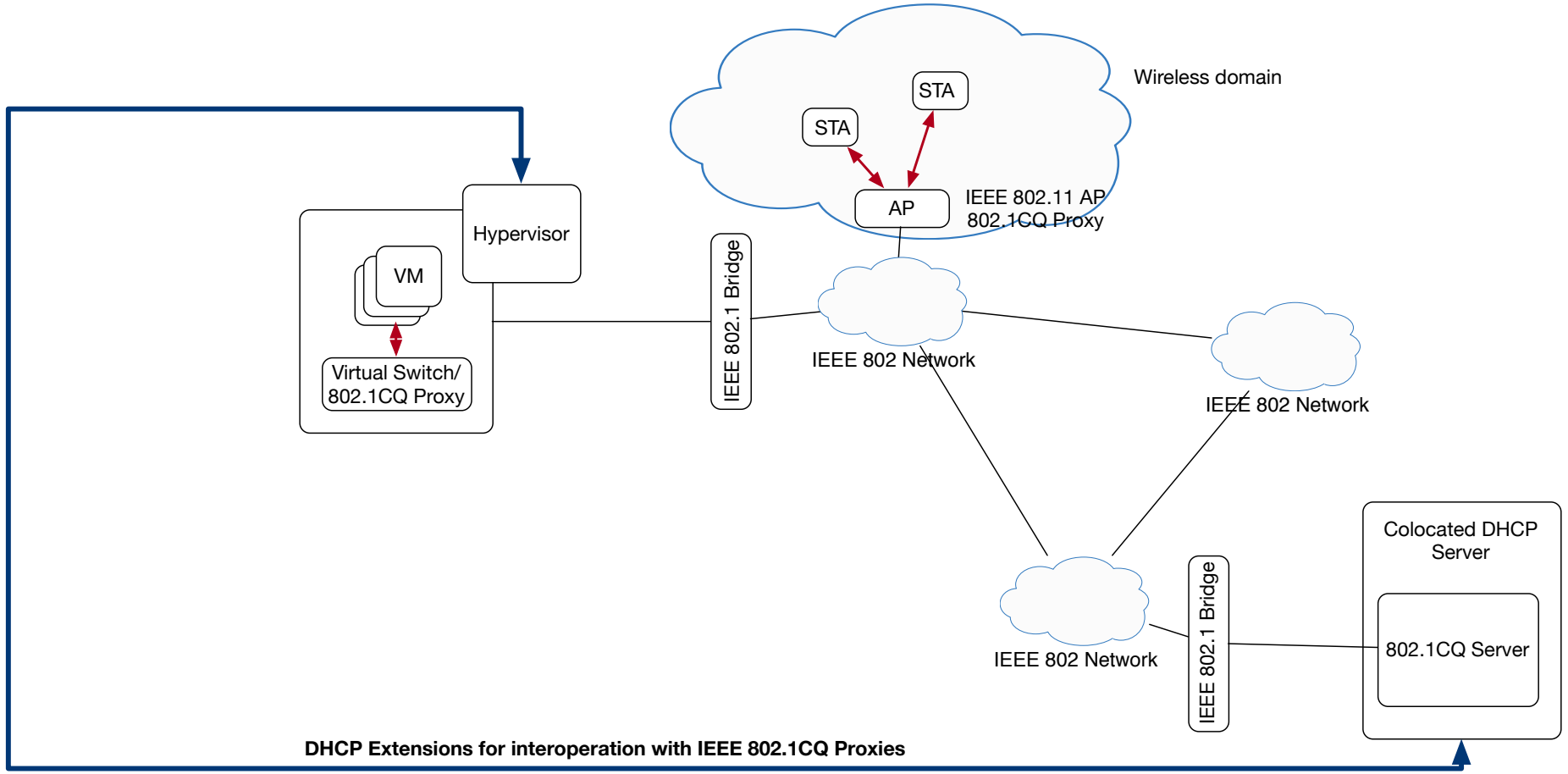
Requirements

- Use-case derived Requirements
  - Stateless/Stateful Assignment of addresses to End-stations
    - 802.11
    - 802.3
    - VMs/Containers
  - Stateless/Stateful Assignment of addresses to Bridges/Aps acting as Proxies
    - Including Assignment of groups of addresses
- Non-functional requirements
  - The protocol SHALL ensure uniqueness of assigned MAC addresses in the scope of its operation.
  - The protocol SHALL ensure the re-assignment of the same MAC addresses during the live time of a session, when re-assignments are taking place. A session is defined as the period of actual or perceived constant connectivity to a network.
  - The protocol SHALL support the assignment of MAC addresses, which are persistently assigned to single stations.
  - The protocol SHALL support a preceding authentication procedure.
  - The protocol SHALL support the derivation of the to be assigned MAC address from the preceding authentication procedure.

Use cases

- We are considering specifically the following scenarios:
  - Virtualisation scenario
    - Hypervisor working as a Proxy, provides assignment of local MAC addresses to the hosted virtual machines/containers
  - WLAN scenario
    - Use of proposed protocol for the assignment of MAC addresses prior to association
  - End-user terminals
    - Standard IEEE 802.3 compliant terminals obtaining Local MAC address upon attachment to the network

Network Model



MAC Address Adquisition Protocol (MAAP)

- Defined in IEEE 1722: IEEE Standard for a Transport Protocol for Time-Sensitive Applications in Bridged Local Area Networks
- It is defined to self-claim multicast addresses
- Protocol based on claiming, probe and defend messages
- Acquisition of addresses:
  - Select an address range from the MAAP dynamic allocation pool.
  - Send a series of MAAP_PROBE protocol data units (PDUs) to determine whether the address range is already in use.
  - Listen for MAAP_DEFEND PDUs indicating the address range is in use.
  - Repeat the above steps until an unused address range has been found.

MAC Address Adquisition Protocol (MAAP)

- It assumes the client to have a unicast MAC address
- Protocol defined as a subtype of IEEE 1722 Ethertype
- Similar to IEEE 802.1CQ mandate, but for multicast only and self-claiming:
  - A block of multicast MAC addresses has been reserved for the use of AVTP.
  - The MAAP specifies a mechanism to allocate multicast MAC addresses dynamically in a specified address range.
  - Any application that uses addresses from the MAAP dynamic allocation pool shall implement the MAAP and MAAP shall be used to allocate these addresses.

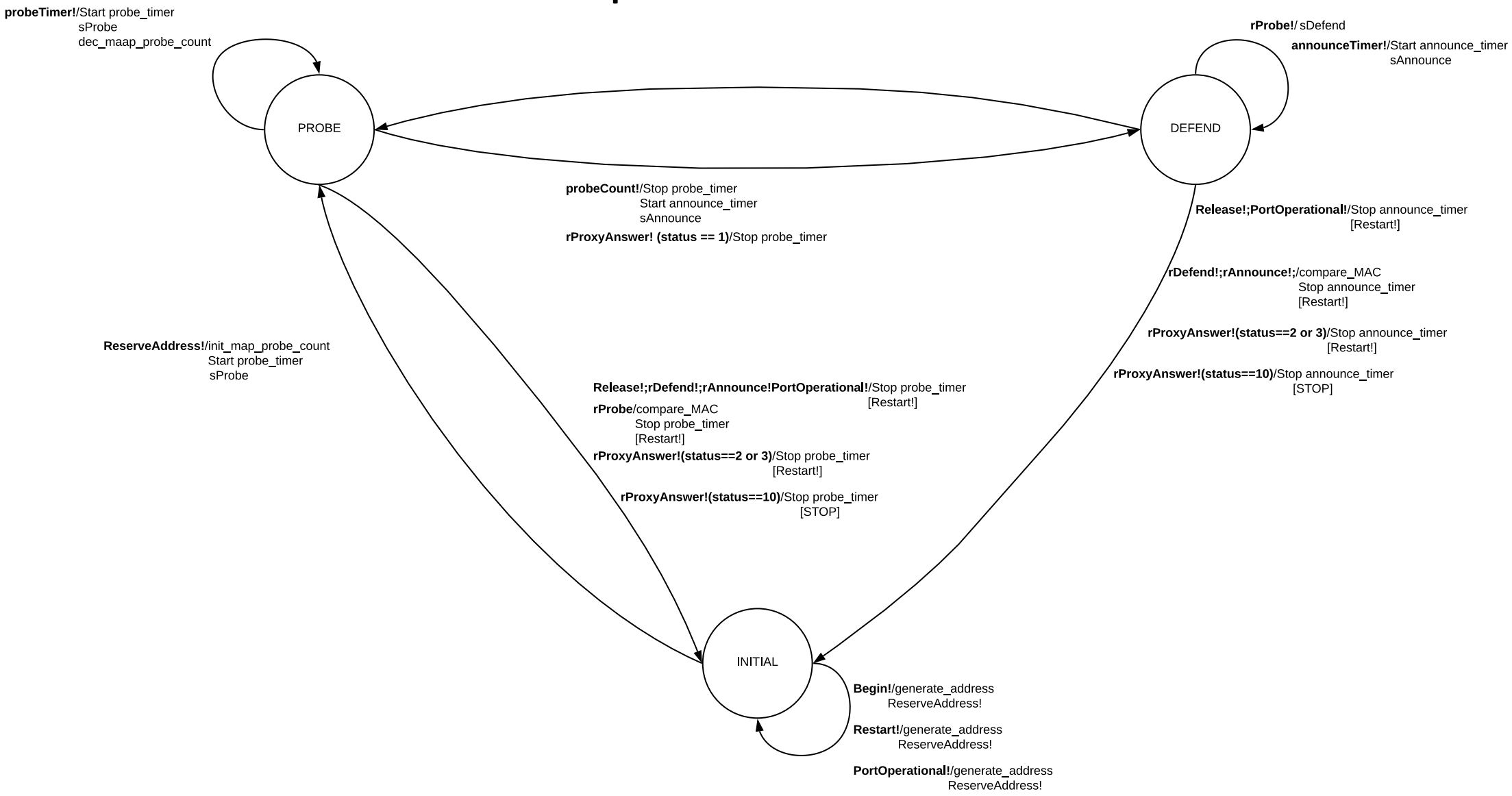
Current IEEE 802.1CQ Proposal

- Multicast and Unicast MAC Address Allocation Protocol (names subject to change)
- MUMAAP has two variants:
  - MASAP: MAC Address Self-Assignment Protocol.
    - MASAP is largely based on IEEE 1722 MAAP protocol
  - MAMAP: MAC Address Managed Assignment Protocol

MASAP Operation

- Following the IEEE 1722 concept, MASAP is based on a PROBE, ANNOUNCE and DEFEND message exchange.
  - After choosing one MAC address, the station will send multiple PROBE messages to advertise the new address allocation
  - If no response is received, the station will go into ANNOUNCE and DEFEND mode, where it advertises its MAC address allocations periodically.
  - In case a PROBE containing an allocation colliding with any of the owned allocations, the station will answer with DEFEND messages.
  - In specific cases, a Proxy in the network can maintain a record of addresses in use and respond to PROBE messages directly.

MASAP Protocol Operation



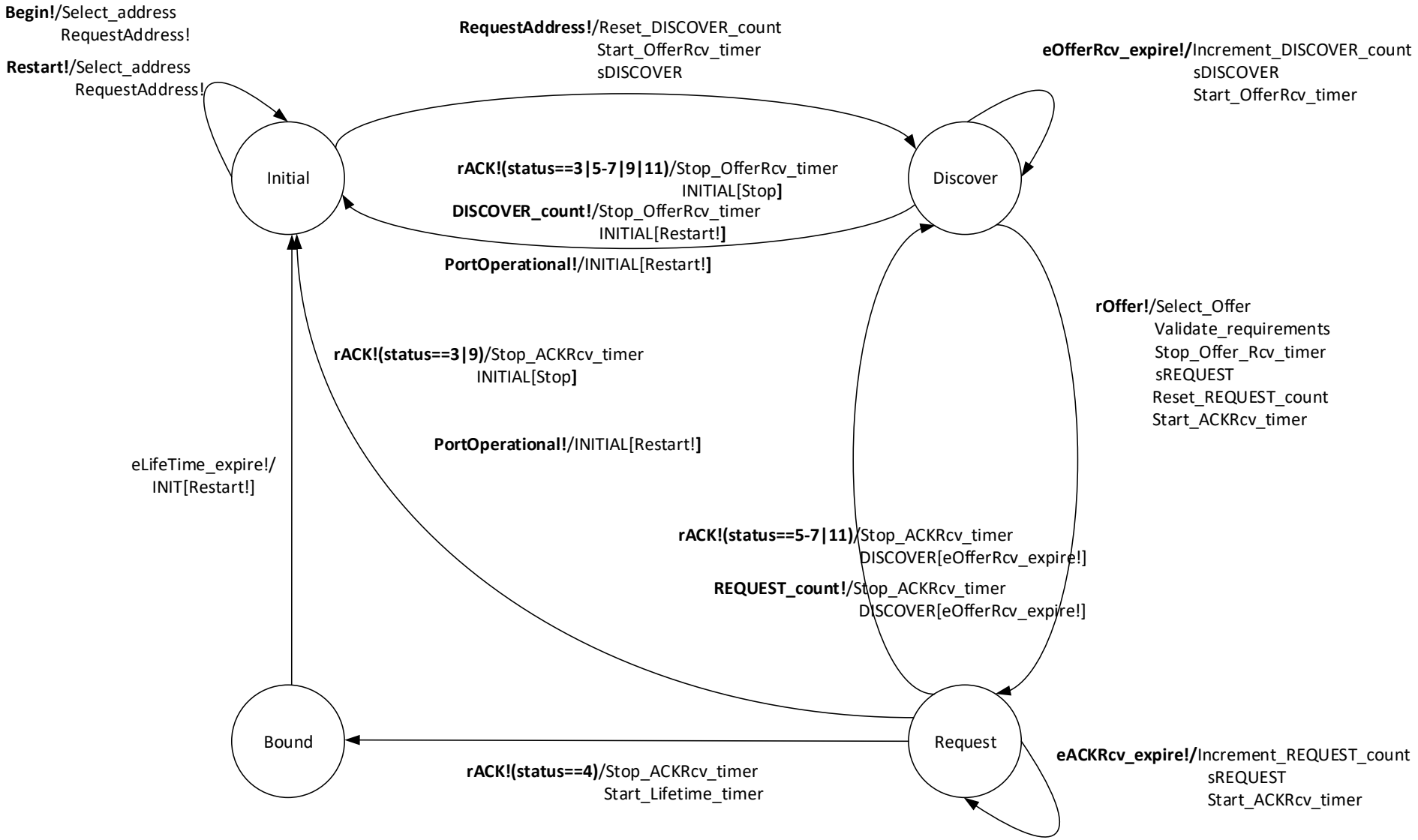
MASAP Message Addressing

- MASAP makes use of the following rules for addressing:
  - Source MAC address for MASAP_PROBE messages will be chosen randomly from a range specified in IEEE 802.1CQ.
  - Source MAC address for MASAP_DEFEND and MASAP_ANNOUNCE messages will use the MAC Address previously assigned or the EUI-64/48 assigned to the station.
  - Destination MAC address for MASAP_PROBE messages corresponds to the multicast address specified in IEEE 802.1CQ.
  - Destination MAC address for MASAP_DEFEND and MASAP_ANNOUNCE messages correspond to the source MAC address of the MASAP_PROBE message.

MAMAP Operation

- MAMAP is used for assign unicast and multicast addresses following IEEE 802c SLAP definition with clients discovering and requested addresses from a MAMAP server(s) or proxy in the network.
- It follows a 4 messages exchange, with DISCOVER, OFFER, REQUEST and ACK messages
- The state machine is based on 4 states: INITIAL, DISCOVER, REQUEST and BOUND

MAMAP Operation



MAMAP Addressing

- MAMAP makes use of the following rules for addressing:
  - Source MAC address for MAMAP_DISCOVER messages will be chosen randomly from the range defined in IEEE 802.1CQ.
  - Source MAC address for MAMAP_REQUEST messages will use the MAC Address previously assigned or the EUI-64/48 assigned to the station.
  - Destination MAC address for MAMAP_DISCOVER messages corresponds to the multicast address specified in IEEE 802.1CQ.
  - Destination MAC address for MAMAP_OFFER and MAMAP_ACK messages correspond to the source MAC address of the MAMAP_DISCOVER message.

Address ranges to be defined in IEEE 802.1CQ

- For the operation of MUMAAP we need the following reserved addresses:
  - Multicast address for self-claiming and managed operation (may be the same?)
  - Range of addresses to select the source of messages (can be randomly chosen from a range)

Message formats

- Both MUMAAP variants share the same message format, under a new Ethertype (or subtype).

0							7	8		10	11				15	16													31
subtype								ver			message_type					control_word													
Cookie																Status												length

MUMAAP Subtype	
MASAP	TBD
MAMAP	TBD

Message formats

Value	Function	Description
0	---	Reserved
1	MASAP_PROBE	Probe MAC address(es)
2	MASAP_DEFEND	Defend MAC address(es)
3	MASAP_ANNOUNCE	Announce MAC address(es)
4	MASAP_PROXY_ANSWER	Answer from proxy regarding Probe messages
5	MAMAP_DISCOVER	Request for a MAC address to a Server
6	MAMAP_OFFER	MAC allocation offer from the server
7	MAMAP_REQUEST	Confirmation of the addresses to be allocated
8	MAMAP_ACK	Confirmation of allocation from server to station or error reporting
8-1024	--	Reserved

Message types

Bit	Name	Description
0	AAI	Bit set to 1: Address in the AAI space requested/provided
1	ELI	Bit set to 1: Address in the ELI space requested/provided
2	SAI	Bit set to 1: Address in the SAI space requested/provided
3	Reserved	Reserved for future use
4	64/48 bits	Bit set to 1: 64 bits address requested/provided Bit set to 0: 48 bits address requested/provided
5	Multicast/Unicast	Bit set to 1: Multicast address requested/provided Bit set to 0: Unicast address requested/provided
6	Infrastructure/Station	Bit set to 1: Message source is Server/Proxy Bit set to 0: Message source is an end-node
7	MAC Provided	Bit set to 1: MAC address is provided Bit set to 0: MAC address is not provided This bit is used by a station providing an already used MAC address as hint to a Server.
8	Station ID provided	Bit set to 1: Station ID is provided Bit set to 0: Station ID is not provided
9	Network ID provided	Bit set to 1: Network ID is provided Bit set to 0: Network ID is not provided
10	Code field provided	Bit set to 1: The message contains a code field Bit set to 0: The message does not contain a code field
8	Specific address type	Bit set to 1: Specific address type information is provided Bit set to 0: Specific address type information is not provided
12-15	Reserved	Reserved for future use

Control Word

Message formats

Value	Description
0	Field not used
1	MAC Range not in use
2	MAC Range in use
3	Re-generate addresses in the given prefix and use MASAP
4	ACK – Assignment accepted
5	Failure – Assignment cannot be completed
6	Failure – Requested quadrant not available
7	Failure – Requested range not available
8	Offer provided
9	Mandatory use of MASAP
10	Mandatory use of MASBAP
11	Parameter problem
12	Offer Provided - Partial fulfillment
13-15	Reserved

Status codes

Type ID	Description
0	Station ID
1	48 bits MAC Address (Range)
2	64 bits MAC Address (Range)
3	Network ID
4	Specific MAC Range
5	48 bits MAC Range in Conflict
6	64 bits MAC Range in Conflict
7	MAC Address Count
8	Lifetime

Message Options