# Proposal for MAC address distribution in IEEE 802.11 networks using the mechanisms of IEEE 802.11aq (Pre-association discovery)

Date:

**Authors:**


| Name | Affiliation | Phone | Email |
|---|---|---|---|
| Antonio de la Oliva | University Carlos III of Madrid, InterDigital | +34916248803 | aoliva@it.uc3m.es |
| Robert Gazda | InterDigital | | |
| | | | |





**Abstract:**
This document proposes and explains how to use standardized IEEE 802.11aq mechanisms for the distribution of MAC addresses.

# Proposal for MAC address distribution in IEEE 802.11 networks using the mechanisms of IEEE 802.11aq (Pre-association discovery)

## Motivation

The IEEE 802.1CQ project [3] is working on a standard specifying protocols, procedures, and management objects for locally-unique assignment of 48-bit and 64-bit addresses in IEEE 802 networks. Peer-to-peer address claiming (called *claiming of addresses*) and address server capabilities are in scope of the CQ standard. This protocol aims to provide methods at layer 2 to automatically assign local MAC addresses in the SAI (Standards Assigned Identifier) space as defined by the recently published IEEE 802c [2]. The SAI space is reserved for use by IEEE 802.1CQ. Two methods of MAC address assignment are in CQ scope: self-assignment (i.e. "claiming of addresses") and server based assignment. In the following, we will define the MAC address assignment service as LAAP (Local Address Assignment Protocol).

The IEEE 802.1CQ project has identified the need for specific MAC address assignment mechanisms for different IEEE 802 based access technologies such as IEEE 802.3 or IEEE 802.11. IEEE 802.11 has special requirements due to the use of the MAC address as part of the association. Therefore, a mechanism to distribute MAC addresses to IEEE 802.11 stations in Pre-Association state is needed.

IEEE 802.11 includes mechanisms to notify stations (i.e. devices) regarding services available in a WLAN network before the station (STA) associates with an Access Point (AP). This is to reduce the overhead of stations connecting and associating with networks, only to discovery that their required services are not present. Specifically, IEEE 802.11aq enables the pre-association discovery (PAD) of services. PAD is an interworking function that enables a STA, prior to association, to discover information related to the services that are available on a WLAN network (also called the Basic Service Set, BSS). PAD methods include: beacon advertisements, service hint / hash, and the generic advertisement service (GAS) / Access Network Query Protocol (ANQP).

This document describes the mechanisms of IEEE 802.11aq that can be used to transport LAAP queries/responses, without any modifying any IEEE 802.11 standardised mechanisms.

In this paper, we present a set of procedures to distribute a MAC address to a station based on IEEE 802.11aq, which can be summarised in the following stages:

- Discovery of the availability of the LAAP service in the network
- Request/Response for a MAC address to the LAAP Proxy/Server

## System Architecture

PAD uses the generic advertisement service (GAS) to:

1. Provide support for a STA's network discovery and selection
2. Provide a communication conduit by a non-AP STA with other information resources in a network before joining the wireless LAN.

The architecture defined by PAD is presented in the following Figure 1 and Figure 2:

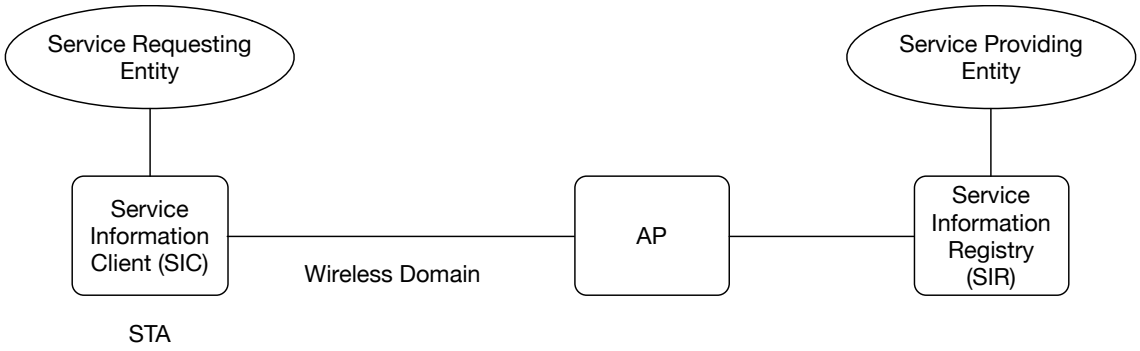


**Figure 1: PAD architecture with direct communication between the AP and the SIR**

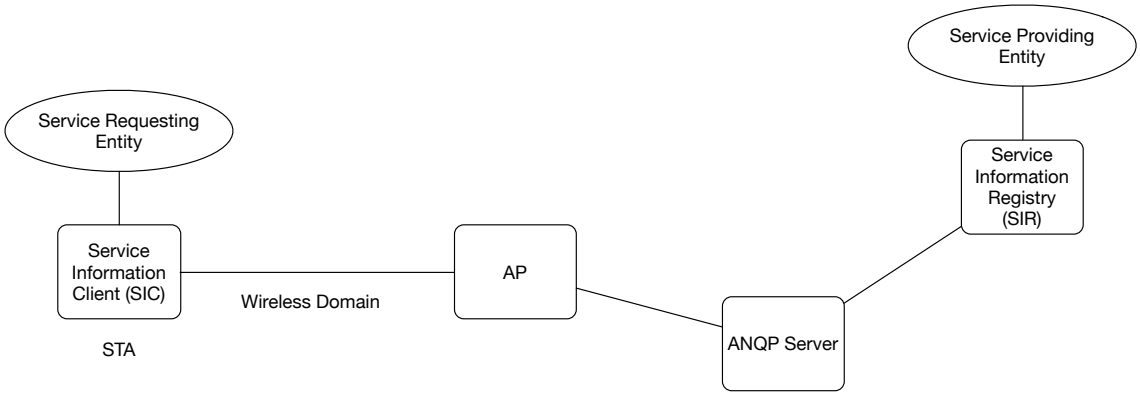


**Figure 2: PAD architecture with indirect communication with SIR through ANQP Server**

A Service Information Registry (SIR) can be either co-located with the AP or separately deployed. The communications between the SIR and the AP, including with the SIR and the ANQP server, are out of the scope of the PAD standard.

The Service Information Client (SIC) and SIR are used to exchange PAD service information. The PAD procedures operate between the SIC and SIR.

The SIR caches information about services that may be reachable via the BSS and therefore may be available to the STA once the STA is associated with that BSS. How the SIR obtains the information about services is outside the scope of the PAD standard.

The SIC initiates service discovery. The SIC exchanges service discovery requests and responses between the SME (Station Management Entity) and applications.

The SME determines whether to use unsolicited PAD or solicited PAD procedures. The SME also composes ANQP requests for solicited PAD procedures.

In the LAAP service scenario, a LAAP Proxy/Server will take the role of Service Providing Entity, which will answer LAAP requests generated by the Service Requesting Entity and transported using PAD mechanisms.

## Discovery of the Availability of the LAAP service in the network

PAD uses different mechanisms for service advertisement, which can be transported in Beacons, Probe Messages or ANQP messages. The mechanisms defined in PAD makes use of two parameters:

- Service Hint: The Service Hint element provides a probabilistic representation of a set of services that are available to the BSS.
- Service Hash: The Service Hash element contains one or more service hashes based on the name of the service.

The Service Hint is formed by a bitmap which contains a bloom filter formed by combining the hash of all the services available in the BSS. Bloom filters are special hashes which have a probability of false positives (the resulting bloom filter indicates a service is available but in reality, it is not).

The Service Hash is the result of applying a SHA-256 hash function to the name of the service. The name of the service must be defined following RFC 6335.

These two elements may be included in the advertising information sent by all APs of the BSS, hence a STA can understand the list of services available, if it knows the names of the services. The main difference between the two mechanisms is that for Service Hint there will be a single field for all services advertised. While for Service Hash there is a separate Service Hash element per Service advertised.

Once the STA understands if a given service may be available, it can query the AP for the specific service or it can even try to communicate with the service provider directly via the GAS protocol and specifically through ANQP.

Therefore, the first step for using the PAD discovery mechanisms is to define new Service Names for the LAAP mechanisms. The Service Names must follow RFC 6335 and register with IANA (Internet Assigned Numbers Authority).

As an example, we could define the following services for LAAP:

- Ieee-8021cq-LAAP-server: This service will indicate there is a LAAP server available.
- Ieee-8021cq-Self-Assignment: This service will indicate this network supports only Self-Assignment (Claiming).
- Ieee-8021cq-Self-Assignment-with-prefix: This service will indicate this network supports Self-Assignment in the context of a given pool of MAC addresses.

These Service Names are used within the Service Hint and Service Hash so a STA can understand if the LAAP service is available in the network and what kind of LAAP mechanism must be used.

The mechanism to build the Service Hash or Service Hint for the above defined service names will be the same one as specified in Clauses 11.25a.4 and 11.25a.5 of IEEE 802.11aq, [4].

These two elements (hash and hint), together or separately are be included in Beacon, Probe response messages, DMG Beacons and Announcement frames.

Once a Service Hint or Service Hash is received by the STA, the STA can compute the hint or hash for a specific Service Name, that it is interested in. If the STA computes a Service Hash or Hint that matches the one received, then the STA knows the service is provided and can proceed to discover information relevant to this service, for example, to learn what is the pool of addresses to be used for Self-Assignment or how to directly contact the LAAP Server.

## Request/Response for a MAC address to the LAAP Proxy/Server

The Generic Advertisement Protocol (GAS) defined in IEEE 802.11 provides transport mechanisms for advertisement services while STAs are in the pre-associated state as well as the associated state. GAS may transport multiple advertisement protocols such ANQP, MIH, EAS, RLQP, etc. If GAS is implemented, ANQP must be supported.

The GAS protocol is a query and response simple protocol. An example GAS flow diagram can be found in Figure 3, on the next page:

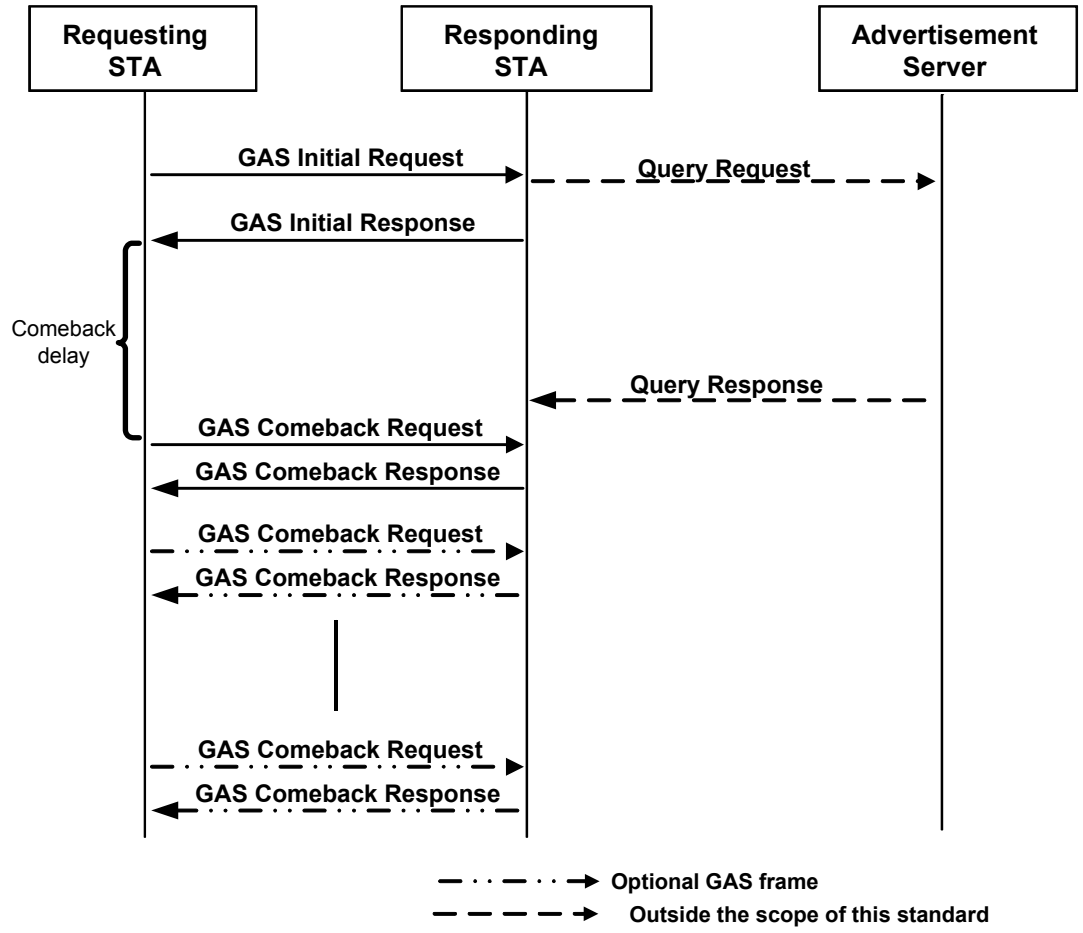


**Figure 3: GAS protocol Flow Diagram**

The GAS protocol is initiated by a STA sending a GAS Initial Request which contains information on the advertisement protocol to be used and other fields to start the conversation such as a Dialogue Token.

Once the AP confirms that the advertisement protocol requested is available, the actual exchange of queries about the services advertised can start (initial queries and responses can be also added to the initial request/responses).

One of the possible protocols transported by GAS is the Access Network Query Protocol (ANQP). ANQP is actually mandatory for all GAS implementations. This TLV-based advertisement protocol allows a STA to obtain from the BSS the following information in a pre-associated state:

| **ANQP-element name** | **ANQP-element type** |
|---|---|
| Query List | Q |
| Capability List | S |
| Venue Name | S |
| Emergency Call Number | S |
| Network Authentication Type | S |
| Roaming Consortium | S |

| ANQP-element name | ANQP-element type |
|---|---|
| Vendor Specific | Q,S |
| IP Address Type Availability | S |
| NAI Realm | S |
| 3GPP Cellular Network | S |
| AP Geospatial Location | S |
| AP Civic Location | S |
| AP Location Public Identifier URI/FQDN | S |
| Domain Name | S |
| Emergency Alert Identifier URI | S |
| TDLS Capability | Q,S |
| Emergency NAI | S |
| Neighbor Report | S |
| Venue URL | S |
| Advice of Charge | S |
| Local Content | S |
| Network Authentication Type with Timestamp | S |
| Service Information Request | Q |
| Service Information Response | S |

**Table 1: ANQP Elements (Q Elements in Query, S Elements in Response)**

From the elements in Table 1, all elements are defined in IEEE 802.11-2016 except the last two, which are defined in PAD and allow to query a SIR directly through a "pass-through" mode of the AP, always in pre-authentication state.

**IEEE 802.1CQ proposes the use of the Service Information Request/Response ANQP Elements for the transport of a LAAP defined protocol for the MAC assignment.**

The Service Information Request ANQP-element contains a generic request for service information associated with the service hash(es) provided.

For IEEE 802.1CQ, LAAP, the STA will use the Hash of the Service Names specified above.

The format of the Service Information Request ANQP-element is shown in Figure 4.

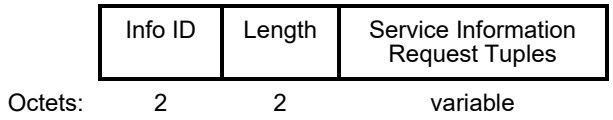


**Figure 4: Service Information Request ANQP Element**

The Service Information Request Tuples field contains one or more Service Information Request Tuple sub-fields. The format of the Service Information Request Tuple subfield is shown in Figure 5.

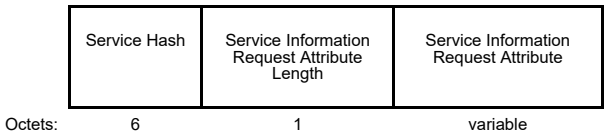


**Figure 5: Service Information Request Tuples**

The Service Information Request Attribute subfield contains a service-specific query. For 802.1cq, it will contain the specific query to the LAAP server in order to obtain a MAC address.

In the same way, the Service Information Response Attribute has a similar format (main difference is the size allowable for the response).

Within IEEE 802.1CQ, we will define a protocol that will be transported as part of the Service Information Request Attribute, which will be able to provide the following functions:

- Request of a MAC address assignment
- Rebind a MAC address
- Delegation of a MAC Address (Response of a previous Request)

In order to do so, the proposal is to define a protocol following a TLV format as follows (as an example):

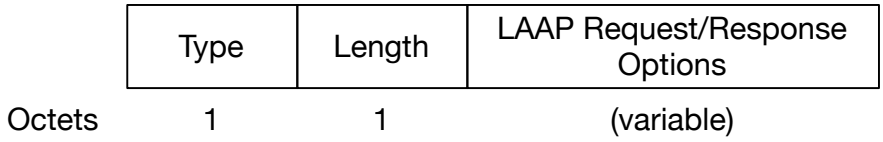


**Figure 6: LAAP Service Information Request Attribute**

The Type Field defines which operation is requested (as an example):

| **Value** | **Description** |
|---|---|
| 0 | Request |
| 1 | Rebind |
| 2 | Response |
| 3-255 | Reserved |

**Table 2: LAAP Service Information Request Type Field Definition**

**The definition of the LAAP Request/Response Options field is within the scope of IEEE 802.1CQ.**

## Overall description of the proposed mechanism

To conclude this document, we present in Figure 7 an overall description of the procedure.

An STA receives a Beacon from an AP supporting a LAAP service. This service is advertised either in the Service Hint or Service Hash.

Since a LAAP service is available, the STA will send a GAS Initial Request including a LAAP Service Information Request Option.

Following the standard GAS procedure, the AP will answer the GAS Initial Request with a GAS Initial Response including a LAAP Service Information Response Option or a GAS Comeback message if the AP needs to contact an external Service entity.

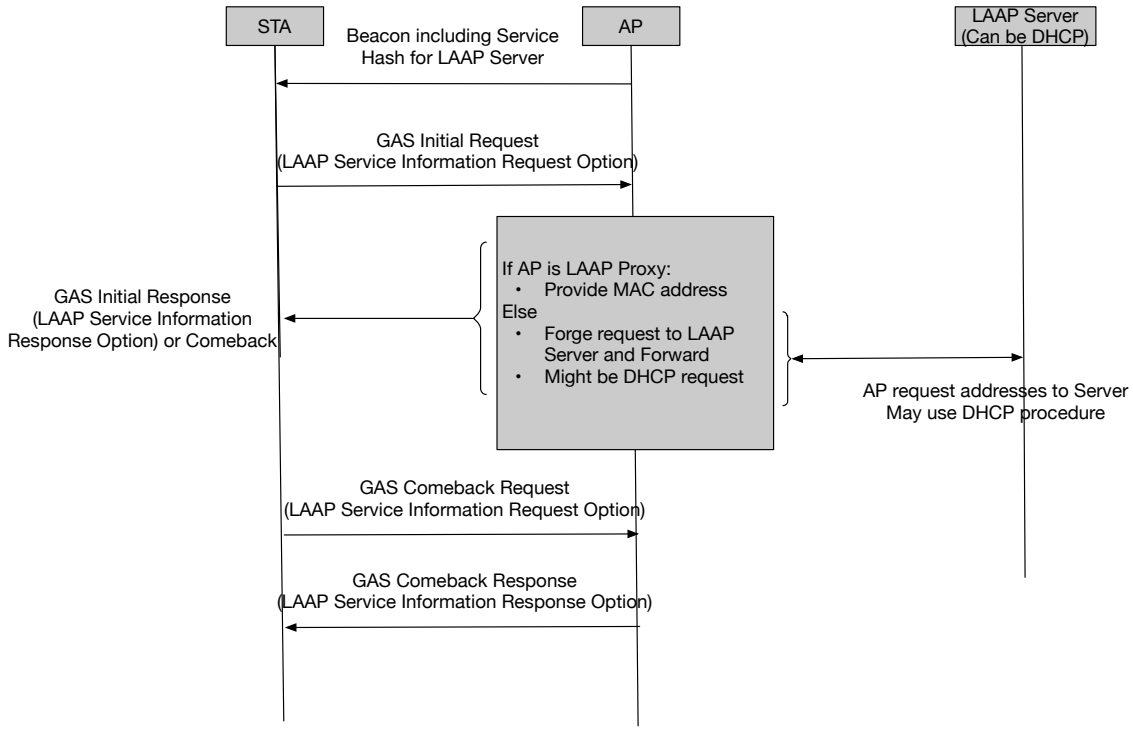


**Figure 7: Global view of the solution**

In this last case, the AP is not a LAAP Proxy and needs to contact another LAAP entity. The AP will request the LAAP Proxy/Server for the MAC address to assign the STA. The procedure to contact the LAAP Server is out of the scope of IEEE 802.11aq and DHCP mechanisms may be used.

# References

[1] IEEE 802.11-2016

[2] http://www.ieee802.org/1/pages/802c.html

[3] https://standards.ieee.org/develop/project/802.1CQ.html

[4] https://standards.ieee.org/develop/project/802.11aq.html