|  |
| --- |
| Local Address Assignment Protocol Requirements |
| Date: 2019-02-05 |
| **Authors:**  |
| Name  | Affiliation  | Email  |
| Maximilian Riegel | Nokia | maximilian.riegel@nokia.com |
|  |  |  |
|  |  |  |
| **Notice:**This document does not represent the agreed view of the IEEE 802.1 OmniRAN TG It represents only the views of the participants listed in the ‘Authors:’ field above. It is offered as a basis for discussion. It is not binding on the contributor, who reserve the right to add, amend or withdraw material contained herein.  |
| **Copyright policy:**The contributor is familiar with the IEEE-SA Copyright Policy <<http://standards.ieee.org/IPR/copyrightpolicy.html>>.  |
| **Patent policy:** The contributor is familiar with the IEEE-SA Patent Policy and Procedures:<[http://standards.ieee.org/guides/bylaws/sect6-7.html#6](http://standards.ieee.org/guides/bylaws/sect6-7.html)> and <[http://standards.ieee.org/guides/opman/sect6.html#6.3](http://standards.ieee.org/guides/opman/sect6.html)>. |

Abstract

This document proposes the addition of fixed address assignments to the list of requirements for P802.1CQ Local Address Assignment Protocol

P802.1CQ Requirements

# Scope

This document provides input to the requirements section of the P802.1CQ specification

# Purpose

Local Address Assignment Protocol provides the capability to dynamically assign arbitrary MAC addresses to IEEE 802 stations. Previously, it was assumed that MAC addresses are configured locally and do not change over the lifetime of a station. Such static assignment led to the assumption that the MAC address wouldn’t be just the temporary endpoint of communications in an IEEE 802 network, but could also be used as permanent identifier for stations.

Aside of technical requirements to provide reliability, security, and scalability to the assignment process of temporary MAC addresses to stations at the begin of network connectivity, the widely deployed secondary usage of MAC addresses as identifier of stations imposes additional requirements to the protocol.

# Background

With the emergence of mobile operating system vendors introducing new functions to the network driver code to make use of randomized MAC addresses for establishing communications over IEEE 802.11 in order to prevent unauthorized tracking of Wi-Fi terminals, operators of Wi-Fi hotspots were facing a number of issues in the operation of their networks. The potential side effects of stepping away from statically configured MAC addresses to dynamic assignments were summarized in a document of the Wireless Broadband Alliance (<https://mentor.ieee.org/802.11/dcn/18/11-18-1579-01-0000-2018-09-liaison-from-wba-re-mac-randomization-impacts.docx>). The following content describing the generic issues of dynamic address assignment is mainly derived from the WBA liaison to IEEE 802.11.

# Common MAC address usage in IEEE 802 network OAM

In IEEE 802, a unique MAC address is assigned to each station. Network operators make use of the MAC address as a reliable unique identifier for the terminal attached to the network. Making use of the MAC addresses as identifier in network operation has a couple of benefits:

* Uniqueness by default
* Provisioned by default
* Common to all types of terminals
* Independent of user or usage of terminals
* Contains hints to the brand and type of terminals
* Resolvable anonymity, i.e. MAC address itself is independent of business contact, but can easily be bound to a business contact.

Due to the favorite nature of the MAC address, it is used for many purposes in network operation:

* Identifier of network usage authorization
During authentication, the authorization of a terminal to make use of network services is bound to the MAC address. The identifier is not only unique to authorization record, but also represents the identifier present in each packet belonging to that authorization. It can directly be used for configuration of packet forwarding and policy functions to deliver the authorized network service.
However, it should be kept in mind that there are no security means in the MAC address to prevent misuse of authorization by another terminal faking its MAC address.
* Identifier of network usage recording
Operators record actual usage of network resources following terminal authentication and authorization. To identify and assign usage records to authorization, the MAC address is often used as it uniquely points to the authorization and is present in each packet belonging to the consumed service.
* Denying network services to single stations
MAC addresses can not only be used for allowing access to network services (authorization), but also for denying access to particular stations. The uniqueness of the identifier ensures that only particular stations are impacted. However, blacklisting of a terminal through its MAC address can easily fooled by locally assigning a different value. Therefore, blacklisting is relying on hard-coded MAC addresses.
* Troubleshooting of networking issues
Due to its presence in forwarded packets as well as in tables guiding the forwarding of packets through bridges, the MAC address is commonly used for troubleshooting of networking issues. It allows to determine whether an issue impacts the network at whole or only single authorizations, and in the case of a helpdesk call of a single user, it allows to track and investigate the network behavior for a single terminal. The brand identifier of the terminal supports the discovery of protocol malfunctions of implementations of particular vendors.

The common usage of MAC addresses in network operation should be considered for the design of the Local Address Assignment Protocol.

# Requirements to maintain common usage of MAC addresses in network operation

The following requirements apply to a local address assignment protocol fulfilling common network operation principles:

* 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.

# Concluding remarks

The described use cases and requirements are not conclusive. Further discussion is necessary to ensure that common IEEE 802 network operation principles are sufficiently supported with locally assigned MAC addresses.