IEEE P802.11
Wireless LANs

|  |
| --- |
| Response to RevCom comment regarding CID concerns on June 9th 2018 |
| Date: 2018-06-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dorothy Stanley | HP Enterprise | 3333 Scott BlvdSanta Clara,CA USA 95054 | +1 630-363-1389 | dorothy.stanley@hpe.com |
| Stephen McCann | BlackBerry Ltd | The Pearce Building, West Street, Maidenhead, SL6 1RL, UK | +44 1753 667099 | smccann@blackberry.com |

Abstract

This document provides a response to the RevCom comment regarding CID concerns on June 9th 2018.

The intent is that this material be used as the basis for further discussion towards establishment of a common understanding between RevCom members, 802.11 members and RAC members of P802.11aq operation and impact.

Hello all,

1. Additional explanatory material is below. Two cases are described, operation without P802.11aq MAC privacy enhancements, and operation with P802.11aq MAC privacy enhancements. This provides a frame of reference and context for the P802.11aq changes.
2. The discussion related to virtual machine address assignment from document 11-18-1032r4 is included.
3. A sample list of WLAN management tools and techniques is also provided. The local network administrator is responsible for administering local MAC address use according to P802-2014 and 802c; using common, well known and established tools, the local address administrator can execute their responsibility. There is no additional address conflict introduced by P802.11aq.

Thanks,

Dorothy

-------------------------------------------------------------------------------------------------------------------------------

Section 1 - Additional explanatory material

Today, without P802.11aq,

1. A local network administrator (LNA) is responsible for local MAC address use and application of policy related to local MAC address use on his or her network. An LNA may choose to have a very restrictive policy, or to apply no specific requirements on use of local MAC addresses.
2. An LNA can choose to use the 802-2014 or 802c-optional-SLAP-AAI (2017) local address spaces, depending on the needs and constraints of his or her network.
3. An LNA might or might not use CID-derived local MAC addresses in their network.
4. An LNA might or might not use virtual machine address assignment in their network.
5. An LNA might or might not use automated or software local MAC address assignment tools. Standardized protocols for automated assignment of MAC addresses are under development, see for example “Link-Layer Addresses Assignment Mechanism for DHCPv6” at <https://tools.ietf.org/html/draft-bvtm-dhc-mac-assign-00>, and <https://1.ieee802.org/dcb/p802-1cq-multicast-and-local-address-assignment/> .
6. The LNA makes decisions on network configuration, and selects and deploys bridges, routers and network elements to instantiate the desired functionality in the network.
7. Consider the following illustrative example. The LNA designs and deploys a network comprised of
	1. A massive number of virtual machines which are assigned CID-derived Local MAC addresses.
	2. There are 4 network segments, imagine perhaps 4 massive datacenters, each of which consumes the entire CID-derived pool of local addresses.
	3. The network design necessarily partitions each network segment from the other segments using a series of routers and gateways.
	4. The LNA uses a custom protocol for automated/software driven CID-based Local MAC address assignment within each network segment.
	5. In addition, the LNA is asked to deploy an 802.11 wireless LAN in each datacenter for technician and staff use for communication needs and for accessing schematics and network operational data.
	6. The LNA designs the WLAN network based on the coverage and throughput requirements, deploying, for example 200 Access Points per datacenter. The LNA uses WLAN network design best practices, instantiating each datacenter WLAN network with 10 WLAN controllers and a smaller number of routers. The WLAN traffic is segmented from the datacenter traffic via the routers.
	7. The technicians using the WLAN network access the WLAN network with both company provided and bring-your-own-devices, including common commercially available Apple, Android (e.g. Samsung) and Windows devices. Traffic from company issued devices and BYOD devices are separated on distinct VLANs at the WLAN APs and controllers.
	8. The example common commercially available devices today each use random MAC addresses pre-association, selected by vendor specific methods, in response to documented device tracking and privacy concerns. For several years now, client device vendors have been implementing and fielding such devices.
	9. Some of these devices also use random MAC addresses post-association, also selected by vendor specific methods, selecting a random local MAC address for the corporate network, which is typically different from the random local MAC address used at the device owner’s coffee shop, bar, hotel visited on vacation, airport and home networks.

Now, let’s consider with P802.11aq functionality

Steps a) through g) 9 are identical to the non-802.11aq case above.

Step h below begins the description of 11aq impacts:

1. With P802.11aq, the common devices and APs support IEEE 802.11aq standard pre-association discovery mechanisms. The client devices can discover for example printer and other services offered by the APs. Both AP and STA must be modified to support 11aq pre-association service discovery; 11aq MAC privacy enhancements apply to the client device only.
2. The LNA can chose to support pre-association service discovery (11aq) in the network or not.
3. The LNA also choses to enable or to disable MAC privacy enhancements on the client devices. Such manageability is not present in non-11aq devices.
4. Continuing the illustrative example above, the LNA decides to enable MAC privacy enhancements on company owned devices. Company owned devices are configured with MAC privacy enhancements enabled, and the MIB variable is set to the default value, indicating that the client device is to use local MAC addresses in the AAI quadrant, as defined in the optional 802c-2017 SLAP. BYOD devices are not configured to enable MAC privacy enhancements, and continue to be segmented on the separate VLAN as before. No additional MAC address conflict with the previously automatically assigned virtual machine local MAC addresses is introduced with the addition of P802.11aq functionality. Using P802.11aq, the 802c defined SLAP mechanism is able to be configured by the LNA for use on client devices.

end of section 1 - Additional explanatory material

-------------------------------------------------------------------------------------------------------------------------------

Section 2 – material from 11-18-1032r4

1. RAC comment: There is a possibility of conflicts with virtual machine local address use and assignment post association. The feared result is that the progress made in getting virtual machines to use CID-based local addresses will be lost, and vendors of equipment implementing virtual machines will return to use of EUIs (EUIs are used for globally unique MAC addresses) for virtual machines. (E.g., vendors assigning 128 EUI-48 to one physical network interface rather than the intended one EUI-48.) The result will be a decrease in the lifetime of the globally unique address space (MA-L, MA-M and MA-S registries). The consequence is a shorter lifetime for the 802-style MAC addressing. The RAC is not aware of any viable way to handle exhaustion of these addresses (e.g., forcing everything to use longer addresses than 48-bits will be much more ugly than was the exhaustion of IPv4 addresses and the ongoing move to IPv6). This impact is not immediate, but is important when trying to sustain the viability of globally unique MAC addresses for 100 years. Goal is to enable software (not local administrator) to assign local addresses to virtual machines.
2. P802.11aq BRC response summary: Possibility of collisions depends on the existing, required ability of a local network administrator to do their job; No additional opportunities are introduced by P802.11aq D14.0 over what is already present in non-P802.11aq compliant systems.
	1. P802.11aq requires network administrator policy configuration of local addresses on stations.
	2. Network administrators of 802.11 based wireless LAN deployments typically segment LANs using routers, and this eliminates possible MAC address duplication. Typically Wireless LAN STAs are isolated on a separate LAN segment from wired STAs.
	3. 802.11 access points include the capability to filter and reject connection requests based on MAC address. Devices using MAC addresses that could potentially conflict with existing LAN equipment can be prevented from connecting to the LAN.
	4. Possibility of collisions depends on Local administrator knowledge of the software address administration being used in the network.
	5. The usage guidelines for EUI and CIDs given in <http://standards.ieee.org/develop/regauth/tut/eui.pdf> state that “Since CID assignments made by the IEEE RA have the X bit equal to 1, an ELI created as an extended identifier from an assigned CID has U/L=1 and is thus, when used as a MAC address, a local address. Local addresses are not globally unique, and a network administrator is responsible for assuring that any local addresses assigned are unique within the span of use. (Uniqueness of local addresses typically does not need to extend beyond a router.) “
	6. No additional opportunities for collisions are introduced by P802.11aq D14.0 over what is already present in non-P802.11aq compliant systems.

Note: There is work underway to define protocols for MAC address assignment, see <https://1.ieee802.org/dcb/p802-1cq-multicast-and-local-address-assignment/> . Nothing in P802.11aq prevents or prohibits use of such protocols when they are defined and available.

End of section 2 – material from 11-18-1032

-------------------------------------------------------------------------------------------------------------------------------

Section 3 – LNA management tools

Available LNA tools and techniques include but are not limited to:

1. Network design and configuration best practices
2. Use of VLANs
3. Use of routers for LAN segmentation
4. WLAN device MIB variables for setting the MAC address (dot11StationID on a per-BSS basis)
5. LNA management of new dot11LocallyAdministeredMACConfig and dot11PrivacyEnabled MIB variables. Management can be via manual configuration in a user interface, Wi-Fi Alliance Passpoint xml based profile, Mobile Device Management systems typically used for cellular/mobile devices, Wi-Fi Alliance Easy Connect, typically used for home and IoT devices.
6. Access Point MAC address blacklist/whitelist.

End of section 3 – LNA management tools

-------------------------------------------------------------------------------------------------------------------------------

**References:**

<http://standards.ieee.org/develop/regauth/index.html>

[Company ID (CID)](http://standards.ieee.org/develop/regauth/cid/index.html)
A unique 24-bit identifier that cannot be used to generate EUI-48 or EUI-64 values. Therefore, the CID is especially applicable in applications where unique MAC addresses are not required.

<http://standards.ieee.org/develop/regauth/cid/index.html>

A CID, like the OUI, is a unique 24-bit identifier. A CID though, cannot be used to generate universally unique MAC addresses. Therefore, the CID is especially applicable in applications where unique MAC addresses are not required. A CID should be applicable in most other cases where an OUI is specified. The CID has been created to reduce the consumption of OUI values.

For more information, please see the tutorial “Guidelines for Use of Organizationally Unique Identifiers (OUI) and Company ID (CID)”.

<http://standards.ieee.org/develop/regauth/tut/eui.pdf> Page 6-7

Since CID assignments made by the IEEE RA have the X bit equal to 1, an ELI created as an extended identifier from an assigned CID has U/L=1 and is thus, when used as a MAC address, a local address. Local addresses are not globally unique, and a network administrator is responsible for assuring that any local addresses assigned are unique within the span of use. (Uniqueness of local addresses typically does not need to extend beyond a router.)