IEEE P802.11
Wireless LANs

|  |
| --- |
| Analysis and repose to 11aq comments related to risk |
| Date: 2018-05-30 |
| 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

In discussions related to P802.11aq, several points related to “risk of address conflicts” and “risk to the Institute” have been raised.

In the text below, these points are listed and a response/analysis provided.

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

1. Comment: “There is a risk of collisions between SLAP [Structured Local Address Plan, defined in 802c-2017] and STA random MAC address use post association. Goal is to enable SLAP to be deployed on a network and not have it be interfered with by stations coming in with random addresses.”
2. Response summary: Risk of collisions depends on the existing, required ability of a local network administrator to do their job; No additional risk is introduced by P802.11aq D14.0 over what is already present in non-P802.11aq compliant systems.
	1. P802.11aq D14.0 requires network administrator policy configuration of MAC addresses on stations associating and joining the LAN. The client station MAC address is set to its Global MAC address by default.
	2. 802.11 networks require a certain amount of provisioning to associate to a network. This includes security policies and credentials. If a network administrator is using the SLAP to administer the local address space on a network, the administrator will also require provisioning of that information on all devices, using the MIB variable defined by 802.11aq, that are allowed on the network via 802.11. In this case there is no conflict.
	3. There are situations where 802.11 networks provide a network access service and the network administrator requires only that an end device/user connect on an SSID to establish network access.  Network administrators that use the SLAP to manage the local address space on their networks will take care, as part of their administrative duties, not to bridge this network access service traffic (traffic from both non-11aq capable client devices, and devices with 11aq dot11MACPrivacyEnabled set to TRUE) onto another LAN segment that operates under the SLAP. Therefore, the only time that there is a possible risk of MAC address collisions is when the administrator is not administering the network correctly.
	4. Risk of collisions depends on ability of the network administrator to do their job.
	5. Network administrators of 802.11 based wireless LAN deployments typically segment LANs using routers, and this eliminates possible MAC address duplication.
	6. No additional risk is introduced by P802.11aq D14.0 over what is already present in non-P802.11aq compliant systems.
	7. P802.11aq compliant systems explicitly require network administrator configuration for local MAC address use; this may increase awareness and reduce any conflicts.
3. Comment: “There is a risk 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 the trying to assure 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. “
4. Response summary: Risk of collisions depends on the existing, required ability of a local network administrator to do their job; No additional risk is 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. Risk depends on Local administrator knowledge of the software address administration being used in the network.
	4. 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.) “
	5. No additional risk is introduced by P802.11aq D14.0 over what is already present in non-P802.11aq compliant systems.
	6. 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.
5. Comment: “An AP might use CID based MAC address values for its BSSID values and unassociated STA(s) might select local random MAC address(es) that conflict.”
6. Response summary: Exceptionally low additional risk; existing CID policies explicitly state that CID derived values cannot be assumed to be globally unique.
	1. The RA guidelines indicate that CIDs are not unique and need to be used in “a well specified context”. See <http://standards.ieee.org/develop/regauth/cid/index.html> under CID: “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.”
	2. See Page 6 <http://standards.ieee.org/develop/regauth/tut/eui.pdf> “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.)”
	3. Assessment of additional risk to CID users– exceptionally low. This risk exists regardless of whether the AP uses a CID-based MAC address for its BSSID (it could also choose a random value).
7. Comment: “Customers of the IEEE RA CID registry are impacted (with corresponding risk to IEEE). It is a concern that implied or expressed values of a CID are compromised if P802.11aq is approved. Concern that a user of P802.11aq would violate implicit and explicit assurances of the CID registry. Need to meet expectations provided by IEEE to CID purchaser. Risk to IEEE of not meeting guarantees that are advertised.”
8. Response summary: Exceptionally low additional risk; existing CID policies explicitly state that CID derived values cannot be assumed to be globally unique.
	1. The RA guidelines indicate that CIDs are not unique and need to be used in “a well specified context”. See <http://standards.ieee.org/develop/regauth/cid/index.html> under CID: “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.”
	2. See Page 6 <http://standards.ieee.org/develop/regauth/tut/eui.pdf> “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.)”
	3. There is no guarantee of uniqueness in CID-based local address usage. IEEE cannot make that assurance when it sells a CID.
	4. Assessment of additional risk – exceptionally low. RA documents indicate that CID derived addresses are not unique and require a network administrator to be responsible for their usage. P802.11aq imposes or adds no additional risk to CID users over risks that are currently documented.
	5. Note: 802.1Q-2014 F.1.2 provides an example of a device which re-uses the same address on all of its network interfaces, and describes mechanisms to mitigate impacts.
9. Comment: “Operation on the wireless medium pre-association conflicts with 802-2014.”
10. Response summary: Conclusion: 802-2014 acknowledges service discovery operations; there is no conflict.
	1. See 4.1 in 802.-2014: “IEEE 802 standards also specify mechanisms to achieve service discovery (e.g., support for Internet or virtual private network service) and session continuity (e.g., a voice over Internet Protocol (IP) or multimedia session) in a heterogeneous networking environment when stations, while either stationary or in motion, have a choice of connecting to multiple access networks.”
	2. See 5.1 in 802-2014: “Each IEEE 802 standard has RMs that are more detailed in order to describe the structure for that specific standard. The RMs for the IEEE 802 standards are given in Annex B.”
	3. See B.2 in 802-2014 for a description of the 802.11 Reference Model.
	4. RAC Chair comment in RevCom dialogue: “The RAC is not concerned about PAD frames”.
	5. Conclusion: 802-2014 acknowledges service discovery operations; there is no conflict.

**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.