**Proposed Resolution of JTC1/SC6 Comments on IEEE Std 802c**

Roger Marks

2018-03-06

1. Background

On 2018-04-02, Andrew Myles wrote:

*The 60 day pre-ballot vote on 802c passed but there were comments from US and China.*

(2) Two comments were submitted; CN1 001 and US 002.

(3) The comments and proposed resolutions are below.

**Comment Number:** CN1 001

**Type:** Ge

**Comment:**

It is suitable to manage the protocol identifiers specified in this proposal by a consolidated and internationally commonly used identifying mechanism.

**Proposed change:**

OID is a flexible, scalable and across heterogeneous systems identifying mechanism proposed by ISO/IEC and ITU-T. OID is commonly used in international standard organizations. It is suggested to use OID for unified management of the protocol identifiers involved in this proposal.

**Proposed resolution:**

IEEE 802 appreciates the review and comments of the China National Body.

<no proposal>

**Comment Number:** US 002

**Type:** Major

**Comment:**

When Ethernet was created with a 48-bit address assigned when the interface was manufactured, it seemed like a nice simple solution that would make installing new devices simple. However, in the intervening 45 years, the Universal MAC address has become a major security problem. The primary properties of an address are that they are only unambiguous within the scope of the layer where they are used and that for larger networks they may be structured to facilitate their use within that layer, e.g. location-dependent, but route-independent. The Universal MAC address has neither of these properties. The size and assignment policy functions more as a device or interface serial number. Consequently, the success of the MAC address and its semantics as a device id allow tracking users and other nefarious purposes beyond delivering Ethernet PDUs to a destination. With increasing compute power and the ubiquity of the network, this has become a serious problem. The MAC address should have one and only one semantic.

Therefore, we recommend that IEEE 802 move toward deprecating the Universal MAC address. If the MAC address can’t be relied on as being globally unambiguous, it can’t be used for nefarious purposes. This could (and to some degree should) be combined with the following actions:

1. The temptation to misuse the MAC address could be countered by moving to the shorter address forms, such as 16 or even 12 bits. This would also obviate the error of using the MAC address as a component of a higher layer address, which has been known as bad engineering since the early 1980s.)
2. An explicit enrollment phase for wired Ethernet, which would not only authenticate the station joining the layer but also assign its address. (802.11 already has an explicit enrollment procedure called association. It should be extended to also assigning an address.)
3. This might lead to defining a more general device-id to be used during enrollment that could be defined by the owner or manufacturer and potentially could be much longer than 48 bits. This device-id would have limited use during enrollment and perhaps not in its assigned form, i.e. encrypted, or as part of a certificate, etc., not in every PDU.
4. The assigned address could be changed periodically as well. Procedures for changing addresses with no effect on data transfer are well-understood and demonstrated.
5. We recommend that IEEE 802 consider making the use of LLC mandatory. Making the SAP fields mandatory would eliminate the need for both the Ethertype field and the VLAN-id field. (The Ethertype field has become an archeology of often long-gone products. The VLAN-id field has been extended by amendment and expanded by the addition of so-called Q-in-Q and MAC-in-MAC standards. Using the SAP fields in LLC as the flow-identifier (which is their role) would be simpler than the Q-in-Q or Mac-in-MAC standards.)
6. Point 5) implies that flows should be explicitly created by the layer above. Note: Allocating flows in this manner does not imply connection or connectionless-mode within the layer. Data transfer may use either mode. It merely allocates the flow between the (N+1)-entities.
7. Also, no identifier shared between the Data Link Layer and the layer above should appear in protocol.

Nota Bene. For points 4, 5, and 6, see the note below.

1. Originally Ethernet was a multi-access media. That meant that any PDU sent on an Ethernet segment passed all stations on the segment. Hence, using an ambiguous address as a multicast address was feasible and even elegant. However as Hubs disappear, Ethernet is now exclusive a traditional network of relays, where multicast requires flooding. IEEE 802 may want to consider moving to the use of multicast protocols (if not already) and a definition of a multicast address as the name of a set of addresses. A more general form that encompasses multicast, anycast, and everything in between has been adopted by the RINA effort, where a ‘whatevercast address’ is defined as the name of a set of addresses with a rule that when the name is resolved, the rule returns elements of the set. (which might be 1, all, or something in between).

Nota Bene: During the development of ISO 7498-3, Naming and Addressing, and later during the development of ISO 8648 Internal Organization of the Network Layer problems were exposed with the definition of (N)-SAP and related concepts. While the proper solution was clear at the time, it was felt that it would be destabilizing to make such major changes at that point. (7498 had progressed to DP in 1980 and was probably at 2nd DP ballot.) Consequently, the problems were patched up by some rather convoluted definitions. (To see what those patches were, see ISO 7498-1 and -3.)

The problem was that the early OSI Reference Model (DP 7498) defined an (N)-address as naming a (N)-Service-Access-Point or (N)-SAP. The (N)-SAP was defined to be at the boundary between the (N)- and (N+1)-layers. Implying the (N)-address was exposed to the (N+1)-entity. This names the path through the layers, which was clearly not a good idea. Because, the OSI definition of a (N)-connection was “an association requested by an (N+1)-entity for the transfer of data between two or more (N+1)-entities,” this implied that a (N)-connection-endpoint, (N)-CEP, was also exposed at the (N)-layer boundary and was defined to be a contained in an (N)-SAP. (See 7498-1, see Figure 7) The CEP-ids distinguished multiple flows through the same address (as it should). Hence, a connection was distinguished within the (N)-layer by the source and destination addresses and the source and destination (N)-CEP-ids. However, this combination of definitions implied that when a flow was created the binding through all of the layers would have to be fixed (resources allocated) before the flow was created. Resource allocation could not occur at establishment time, i.e. no late binding. This is clearly not a desirable property.

This also meant that there was no term for the relation created by the exchange of (N)-PDUs between (N)-entity-instances. Such a term was needed for two reasons: 1) not all behavior of the (N)-protocol is visible to the (N+1)-layer. The effect of these functions is not a property of the (N)-connection, but of this other relation. 2) at the Application Layer there was only this unnamed relation. Hence, a new term, (N)-association, was defined as the relation between two (N)-entity-instances to represent the shared state of the flow. (Basically, the definitions are backwards. (N)-connection should have the definition of (N)-association and vice versa.) If these definitions are used as originally defined then not only is late binding and dynamic resource allocation not possible, but simple solutions to multihoming and mobility are thwarted as well.

Aspects of the IEEE 802 architecture reflect these misconceptions and would be greatly improved if IEEE 802 rectified them as described below.

These problems and their solution were further confirmed by the work on ISO 8648, where because the (N)-address was exposed at the layer boundary, routing on the (N)-address would have been route-dependent. It was known that relaying in the (N)-layer had to be based on the (N)-entity or (N)-subsystem (to solve multi-homing), 8648 defines relaying, or forwarding, to be based on the Network-entity-title, not the Network-address, i.e. where N = 3.

Richard Watson’s proof that the necessary and sufficient conditions for synchronization for reliable data transfer implies that port allocation and synchronization should be decoupled, (or put another way, decoupling the (N)-SAP-ids from (N)-CEP-ids.) This further confirms the corrections to the model. As well as the fact that various known attacks on TCP, which doesn’t separate them are successful, while the same attacks on Watson’s delta-t are not successful further confirms the structure below.

The appropriate solution would have been:

(N)-address – names the (N)-entity or (N)-subsystem and is unambiguous within the scope of the layer.

(N)-CEP-id – names the (N)-entity-instance the state of a (N)-flow and is unambiguous within the (N)-subsystem.

(N)-SAP-id – names the (N)-SAP (at the layer boundary) and is unambiguous with the scope of the (N)- and (N+1)-subsystems.

An initiating (N+1)-entity requests data transfer with a destination (N+1)-entity. It is the task of the (N)-layer to make the mapping from (N+1)-entity-title to (N)-address and establish the (N)-connection between the (N)-entities. The local (N)-layer creates the mapping between the (N)-SAP-id and (N)-CEP-id. The (N)-CEP-ids are carried in protocol. The (N)-SAP-ids are not. These definitions allow late binding, and greatly simplify multihoming and mobility.

We strongly suggest that IEEE 802 move to adopt the 8 recommendations above and the architecture definitions described here.

**Proposed change**:

1. The temptation to misuse the MAC address could be countered by moving to the shorter address forms, such as 16 or even 12 bits. This would also obviate the error of using the MAC address as a component of a higher layer address, which has been known as bad engineering since the early 1980s.)
2. An explicit enrollment phase for wired Ethernet, which would not only authenticate the station joining the layer but also assign its address. (802.11 already has an explicit enrollment procedure called association. It should be extended to also assigning an address.)
3. This might lead to defining a more general device-id to be used during enrollment that could be defined by the owner or manufacturer and potentially could be much longer than 48 bits. This device-id would have limited use during enrollment and perhaps not in its assigned form, i.e. encrypted, or as part of a certificate, etc., not in every PDU.
4. The assigned address could be changed periodically as well. Procedures for changing addresses with no effect on data transfer are well-understood and demonstrated.
5. We recommend that IEEE 802 consider making the use of LLC mandatory. Making the SAP fields mandatory would eliminate the need for both the Ethertype field and the VLAN-id field. (The Ethertype field has become an archeology of often long-gone products. The VLAN-id field has been extended by amendment and expanded by the addition of so-called Q-in-Q and MAC-in-MAC standards. Using the SAP fields in LLC as the flow-identifier (which is their role) would be simpler than the Q-in-Q or Mac-in-MAC standards.)
6. Point 5) implies that flows should be explicitly created by the layer above. Note: Allocating flows in this manner does not imply connection or connectionless-mode within the layer. Data transfer may use either mode. It merely allocates the flow between the (N+1)-entities.
7. Also, no identifier shared between the Data Link Layer and the layer above should appear in protocol.

Nota Bene. For points 4, 5, and 6, see the note below.

1. Originally Ethernet was a multi-access media. That meant that any PDU sent on an Ethernet segment passed all stations on the segment. Hence, using an ambiguous address as a multicast address was feasible and even elegant. However as Hubs disappear, Ethernet is now exclusive a traditional network of relays, where multicast requires flooding. IEEE 802 may want to consider moving to the use of multicast protocols (if not already) and a definition of a multicast address as the name of a set of addresses. A more general form that encompasses multicast, anycast, and everything in between has been adopted by the RINA effort, where a ‘whatevercast address’ is defined as the name of a set of addresses with a rule that when the name is resolved, the rule returns elements of the set. (which might be 1, all, or something in between).

We strongly suggest that IEEE 802 move to adopt the 8 recommendations above and the architecture definitions described here.

**Proposed resolution:**

IEEE 802 appreciates the review and comments of the U.S. National Body.

IEEE observes that this comment appears to not be directed at the proposed amendment, IEEE Std 802c, but at the baseline document to be amended, ISO/IEC/IEEE 8802-A:2015 (“Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Part A: Overview and architecture”). The comment proposes significant changes to that architecture. Because the entire family of ISO/IEC/IEEE 8802 standards is dependent on that architecture, such changes would have significant implications throughout the family of standards.

IEEE 802 recognizes that some of the changes incorporated into the standard by means of the amendment could enable further future revisions with the potential to achieve some of the stated aims with minimal disruption to the family of standards and the ecosystems built thereon. For example:

* Proposed change (1) suggested shorter addresses, such as 16 or 12 bits. IEEE Std 802c specifies the use of 48-bit address form known as the Extended Local Identifier (ELI). The first 24 bits of the ELI are assigned as a unique Company ID (CID), with the remainder specified as an extension by the CID assignee or by a protocol designated by the CID assignee. This address form could readily support the proposal for shorter addresses without minimal effect on backwards compatibility. This would also support other proposed changes, such as proposed change (4).
* Addresses assignment protocols, as suggested in proposed change (2), are in development within IEEE 802 through the P802.1CQ project, based on the amendment proposed to ISO/IEC as IEEE Std 802c.
* The comment also recommends deprecation of the Universal MAC address. We believe that such a change is neither warranted nor advisable but would be highly disruptive to the industries using the 8802 family of standards. However, we note IEEE Std 802c provides means to coordinate the use of alternative address space (the local address space) by specification of the Structured Local Address Plan (SLAP). This development would offer alternative means to provide for addressing in the local space, maintaining backward compatibility, for circumstances in which universal addresses are perceived as problematic.

For these reasons, many of the goals expressed in the comment would best be served by approval of the proposed amendment.