IEEE P802.11

Wireless Access Method and Physical Layer Specification

How Far Should an ESS Extend?

Michael Fischer
Digital Ocean, Inc.
4242–3 Medical Drive
San Antonio, TX 78229

Telephone: +1–210–614–4096
Facsimile: +1–210–614–8192
email: mfischer@CHILD.com

Abstract

The "basic service set" (BSS) and "extended service set" (ESS) are two of the oldest and most stable concepts in the 802.11 standard. Examining these concepts in terms of the new MAC state machines (clause 6.7 of D2.0 or document 95/014r2) shows that BSS is an appropriate concept for defining the scope of a network segment for wireless media, and is adequately supported by MAC services. However, ESS is shown to be a composite of three, distinct concepts: local coverage extension, wired network integration, and remote coverage extension; none of which are adequately specified.

Clause 1 of this submission proposes that the definition of ESS, for all existing usage in the draft standard, be narrowed to include only the first two of these three concepts, and identifies many of the underspecified functions specific to these concepts. For any remaining cases where a term is needed to refer to the third extended service concept, the this submission suggests "more extended service set" (MESS).

Clause 2 of this document proposes an escape mechanism which can be used by 802.11 distribution system services to perform transparent integration of non–802 LANs that convey LLC–visible information in their MAC headers (e.g. the protocol type codes in type 2 Ethernet). In the absence of a standardized mechanism for this purpose, portals to such LANs would either be impossible (in an interoperable form), or would limit their ESS to running a single higher–layer protocol stack. The proposed mechanism solves this problem in a manner where the added overhead applies exclusively to the MSDUs which convey the problem protocols.

Category: "things that are broken, but do not appear so due to vague specification"

This submission identifies a portion of the MAC that is inadequately specified, and suggests some of the appropriate changes to the specifications. This submission also recommends elimination of some (hypothetical) functionality because providing the required details appears to be of marginal benefit, and to be outside the charter of 802.11 (possibly outside the charter of IEEE 802). By eliminating this degree of freedom, the path is cleared to solve a more practical problem, relevant to significant numbers of existing wired network users, thereby removing an obstacle to their attachment of 802.11–based products to their existing networks.

CLAUSE 1 — Revised Service Set Definition for Reasonable Limit to ESS Extent

The BSS is the 802.11 concept which provides the logical mechanism to permit a wireless LAN to have many of the same operational properties as a single segment of a wired LAN. These characteristics of the wired LAN are inherent, due to their use of wired physical media, which limit each transmission to a single segment of network cable, allow almost all transmissions to be received by each of the stations attached to the network cable, and achieve a much lower bit error rate than wireless media. The fundamental mechanisms which delimit the operational boundaries of each BSS are the BSSID, a code which permits stations to filter received frames, accepting only those from the correct "logical wire;" and the access point (AP), a station in the BSS which provides access to distribution system services (DSS), thereby allowing communication with LAN stations outside of the BSS. The AP is also the entity within each BSS that provides functions peculiar to the wireless environment, such as power management and authentication.

The ESS is the 802.11 concept which permits a plurality of BSSes to be connected into a single logical network, and to be integrated with other (wired) LANs. The basic characteristic of the ESS is the connection of a plurality of network segments into the "extended" logical network. In addition, the DSS within the ESS support mobility, permitting portable stations to move among different BSSes of the ESS in a manner transparent to other stations within the ESS with whom the mobile stations are exchanging LPDUs. The fundamental concepts which delimit the operational boundaries of each ESS are the ESSID, a code which permits stations to identify the ESS to which a given BSS belongs, and the distribution system medium (DSM), which connects all the DSS entities within the ESS.

Separating Extended Service Set Concepts

The BSS is a fairly "simple" concept, with all functions existing either at all stations or at the AP. However, the ESS is much more complex, with functions scattered among stations, APs, Portals, and DSS entities which may be located elsewhere on the DSM (plus the added complexity of both wired and wireless DSM connections, the latter referred to as "wireless distribution system" or WDS). When attempting to clarify some nebulous ESS specifications, it becomes apparent that the ESS is a composite of at least three, distinct concepts, which do not necessarily share common functional characteristics nor physical scope. Each of these three concepts is discussed below:

A) Local Coverage Extension

The most important component of the ESS concept is a mechanism to enlarge the area served by a single wireless network. The physical characteristics of certain wireless media, as well as regulatory constraints on radiated power, limit the coverage of many BSSes to areas smaller than are typical for "local area" connectivity, as well as smaller than the coverage areas needed by the users of many wireless networks. The direct solution to this problem is to connect a plurality of BSSes to a common distribution system in order to cover a sufficiently large physical area to qualify as a "local area" network. The resulting ESS composed of directly connected BSSes is similar to a set of wired network segments connected by PHY repeaters and/or by MAC bridges. The major function present in a locally–extended ESS but not available from a set of bridged LAN segments is BSS–transition mobility that is transparent to other end–stations that are communicating with the mobile station.

B) Wired Network Integration

The functional concept of "integration" and the corresponding structural concept of a "portal" are unique to wireless LANs. For collections of wired network segments, there is no reason to distinguish between "extension" and "integration" because both involve an identical PDU relay function — specified for 802 LANs in 802.1d (MAC Bridges). When connecting wired network segments to an 802.11 distribution system, there are additional considerations because of the mobility and power save mode support in the 802.11 MAC. While the integration functionality at each portal includes many of the same address filtering functions as a MAC Bridge, integration services must also deal with addressed stations which may move (BSS mobility transitions) while MSDU exchange is in progress, as well as addressed stations which are not continuously able to receive MSDUs (power save operation), neither of which are functional attributes of destination addresses in the conventional (MAC Bridge) model of multi–segment LAN extension.

C) Disjoint Coverage Extension

The D2.0 draft states that "the DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity" and that "nothing is assumed by 802.11 about the relative physical locations of the BSSs in {an ESS}." These statements allow the possibility of distribution systems which include routers, wide–area links, and other non–LAN elements within a single ESS. An extended network which includes these elements is "disjoint" from the point of view of any directly–connected of MAC–layer entities, as well as (generally) being physically disjoint due to the existence of BSSes of the ESS at physically distinct sites. These sites are "distinct" due to physical separations by distances substantially greater than the maximum scope of "local area" network coverage — there is nothing about the "local coverage extension" concept listed above which requires continuous or uninterrupted spatial coverage, just a limitation of any multi–BSS coverage which exists under that concept to the confines of a single "local area."

Problems With Allowing Disjoint Coverage Extension in an ESS

There are several, severe problems with using a single structural entity — the ESS — to cover all three of the concepts listed above. The combination of local coverage extension and wired network integration is quite appropriate. Local coverage extension is what allows 802.11 to offer a local area network instead of "sub–local area" network, while wired network integration provides the functionality not present in 802.1d MAC Bridges but necessary when connecting conventional LANs to WLANs due to the unique behaviors of certain WLAN stations. Therefore, including these two concepts in the ESS are non–problematic. All of the problems derive from the inclusion of disjoint coverage extension:

1. The presence of routers (which operate at the network layer) within the distribution system creates the possibility that network layer connectivity does not match data link (MAC) layer connectivity. Unless routers are aware of mobility transitions, frames could be mis–directed without the mis–direction being detectable or correctable. It would be a violation of protocol layering for MAC entities to generate routing table update messages (RIP, OSPF, etc.). It would be a different, but equally serious, violation of protocol layering for a MAC entity, such as distribution services at an AP, to inspect what it believes are the network layer addresses in the payload of an undeliverable MSDU, as would be necessary for an "old AP" to forward mis–directed frames in a disjoint–coverage ESS. Even if these violations of protocol layering were felt to be "acceptable" (which ISO would not), the resulting implementation would only be restricted to specific, predefined higher–layer protocols.

2. Allowing the distribution system to extend outside of MAC/PHY layers creates unknown risks to both the privacy and the authentication mechanisms. As long as the DSM consists solely of directly connected wired LAN segments and wireless segments using WEP, MSDUs and authentication/association state information transferred over the distribution system are as secure as the wired network (assuming procedures and higher layer mechanisms are equal). When entities outside of the MAC/PHY layers are involved in MSDU transport (for an ESS which uses anything more secure than open system authentication), either reassociations must be prohibited or a secure mechanism for exchange of station state between distribution service entities needs to be added to the draft standard.

3. The presence of wide area links within the distribution system creates the possibility of unbounded delivery delays over the DSM. At best, this increases the buffering requirements at APs (especially if the wide area links use data rates slower than the 802.11 PHY data rates); at worst, this allows higher layer protocol time-outs to occur while MSDU delivery is underway. Even worse, if distribution services must allow for the possibility of wide area links, changes to authentication and association status anywhere within the BSS have to be communicated to the rest of the APs as these changes occur, otherwise reassociation could be delayed sufficiently long to cause higher–layer time-outs on sessions at the station waiting to reassociate. The association information exchange architecture (disseminate vs. query) is not currently specified and is not nearly as constrained by higher layer expectations when disjoint coverage extension is excluded.

4. The presence of point–to–point links, such as frame relay, or virtual circuit switched links, such as ATM, within the distribution system can create a requirement for explicit knowledge of infrastructure topology at each site which has an active distribution services entity. There is no such requirement when using only local, packet–switched links using the MAC address space.

5. Whether or not the Inter–Access Point Protocol (IAPP) is defined as an exposed interface in the initial version of the 802.11 standard, this interface is a location in the WLAN architecture where mixed–vendor interoperability is possible, and where standards may be worth defining. If the ESS is allowed to include network layer entities (e.g. routers) and/or non–LAN segments, the IAPP can never be part of 802.11, because the IAPP standard would have to specify the behavior of entities which lie outside the charter of IEEE 802.

6. There are attempts underway to define virtual LAN (VLAN) standards within IEEE 802. If these efforts are successful, the VLANs will virtualize station location over a set of MAC/PHY (e.g. bridgeable) segments, not across unrelated MAC segments (where routing is necessary for higher–layer transparency). Since support for wireless mobility is one of the major advantages of a VLAN, the fundamental "big" unit of 802.11 aggregation needs to be able to integrate directly as an element of an 802 VLAN. If we fail to limit the maximum extent of an ESS now, it will be necessary to amend 802.11 to add an unit of coverage extension which excludes disjoint–extended networks once VLAN standardization is completed.

7. The primary operators of networks sufficiently large to have any reason to consider disjoint–extended service sets are large corporations, educational institutions, and government agencies. The network administrators at such organizations are already dealing with the management of heterogeneous collections of physically scattered, interconnected LANs, and are already supporting (non–real–time) mobility transitions between those LANs for mobile workers. These organizations, which are among the most likely customers for significant quantities of 802.11–conformant WLAN equipment, are the least likely to want a portion of the WLAN structure which extends above the data link layer and/or onto non–LAN media. In fact, feedback this author has received from network administrators at more than one organization of this type is that they want 802.11 networks to fit the same structural model as wired LANs. These user needs require local coverage extension (at least for the existing PHYs) and wired network integration, but specifically do not include disjoint coverage extension. It is senseless to complicate our standard to provide functions that the target users do not want and are unlikely to use even if available in 802.11 products.

Recommended Changes to Extended Network Definitions

A simple solution to these manifold problems is to redefine "Extended Service Set" to include only the local coverage extension and wired network integration concepts, and to exist strictly within the MAC and PHY layers of the ISO reference model. By doing this, all of the subsequent discussions of distribution systems and services can be left unmodified, because the extent of the service set has been properly bounded. An appropriate definition, derived from the text in section 1.1 of the D2.0 Draft, is presented below:

Extended Service Set (ESS)

A set of one or more ~~interconnected~~ Basic Service Sets and zero or more integrated LANs, connected to a common Distribution System, allowing them to appear ~~which appear~~ as a single Basic Service Set to the logical link control entity ~~layer~~ at any station associated with one of those BSSs and at any station attached to one of those integrated LANs. The DSM of an ESS shall be comprised solely of 802 LAN segments (including wireless LAN segments), and any physical layer repeaters and/or 802.1d MAC Bridges necessary to interconnect those LAN segments.

There is no reason to prohibit the use of a common ESSID for a set of ESSes (new definition, above) connected using routers and/or wide–area links. It is probably possible, under certain circumstances, to implement distribution services for such a network in a manner which provides many of the normal ESS functions within the disjoint–extended environment (especially if the inter–ESS links are much faster than the 802.11 PHYs). However, this construct needs a distinct name, so readers of the standard, as well as users of such a configuration, are aware of the different limitations (more properly, boundary conditions) which pertain to a disjoint–extended network. An appropriate name for this concept is "more extended service set," as defined below:

More Extended Service Set (MESS)

An Extended Service Set in which the Distribution System operates above the data link layer and/or in which the DSM includes one or more routers, gateways, or non–LAN segments. Some distribution system services may be unavailable between arbitrary pairs of stations in an MESS, and some mobility transitions may be impossible between arbitrary BSSs in an MESS.

The problems with the prevailing scope of the ESS concept can be solved by replacing the definition of ESS in section 1.1 of the D2.0 draft with these two definitions. These definitions also need to be propagated to the corresponding paragraphs in section 2 for internal consistency.

CLAUSE 2 — Ancillary LLC Information Encapsulation Mechanism

For portals to function properly, all information being exchanged between peer LLC entities must be conveyed properly across both the distribution system medium (DSM) and wireless medium (WM) of the ESS, and to be handled without loss at the points where the information enters and exits the ESS, whether those points are LLC interfaces at stations within the ESS or integrated LAN interfaces at portals. For intra–ESS communication, and portals which integrate other 802 LANs, this is relatively simple to achieve. All of the 802 MAC protocols fully separate MAC framing information and LLC information, treating the LPDU as the MSDU payload. Unfortunately, certain types of non–802 LANs do not obey this strict separation of LLC–visible information from MAC–specific information. The result is potential ambiguity, which can cause insertion or removal of information from the LPDU when translating between different LAN types. Rather than precluding integration of certain non–802 LANs (which is the approach taken by FDDI), 802.11 can provide unrestricted integration of these LANs by adopting the mechanism described below. A further advantage of this mechanism is that the added overhead of integrating the "ill–behaved" LANs applies only to the MSDUs which convey LPDUs for those LANs, leaving normal MSDUs of 802.11 and other 802–type LANs unaffected.

Definition of the Problem

The principal example of the integration problem caused by ill–behaved, non–802 LANs the inclusion of a protocol type code in the MAC header. This protocol type code is used at the destination station to select the correct higher–layer protocol handler for the LPDU, and is therefore LLC layer information. In order for 802.11 distribution systems to integrate LANs with these sorts of protocols, there must be a way to indicate the presence of such information, and to encapsulate the information in a manner which is unambiguous to 802 LANs, including 802.11 station functionality. The most common instance of an ill–behaved, non–802 LAN is type 2 Ethernet, which places a protocol type code in the MAC header field which 802.3 Ethernet uses for the frame length. (Another non–802 LAN which has a protocol type code in its MAC header is ARCNET.) A portal which integrates an 802.3 LAN cannot treat the length field as part of the LPDU, because to do so would add two, non–LPDU octets to the beginning of the MSDU passed to LLC at the destination. On the other hand, a portal which integrates a type 2 Ethernet LAN cannot discard the type code, because some protocol stacks layered above type 2 Ethernet, notably TCP/IP, rely upon the contents of this field reaching the destination station. The simple solutions to preserving this information have the side effect of limiting the ESS to supporting only one type of higher layer protocol, which is not the intent of 802.11 LAN integration.

Proposed Solution

A general solution to this problem is to use the high–order bit of the subtype field of the data frame type. This bit is =0 for all eight currently defined data subtypes. Under this proposal, this bit being =1 would indicate the presence of encapsulated LLC information in the MSDU payload. The three low–order bits of the subtype field would be interpreted as currently defined, independent of the state of the high–order subtype bit. This permits MSDUs with encapsulated LLC information to be transferred in an identical manner to normal MSDUs, using either distributed or point coordination functions. When this high–order data subtype bit is =1, the MSDU payload begins with an element that encapsulates the ancillary LLC information. When present, encapsulated information element is located just before the conventional LPDU, and is considered part of the MSDU payload. Therefore, if WEP is used on a frame with ancillary LLC information, the IV field is located between the MAC header and the encapsulated information element.

The general format of the enacapsulated information element, and the specific layout and values for use with type 2 Ethernet, are shown below in Figure 1. The first octet contains a type code indicating the type of encapsulated information. Currently a information type value of 0 is defined to mean a protocol type code, and all other type values are reserved. The second octet contains the number of octets in the remainder of the element, which is always an even number. If necessary, a pad octet is added at the end of the encapsulated information to maintain even octet alignment for the remainder of the MSDU payload. For information type 0, the information length is 2.

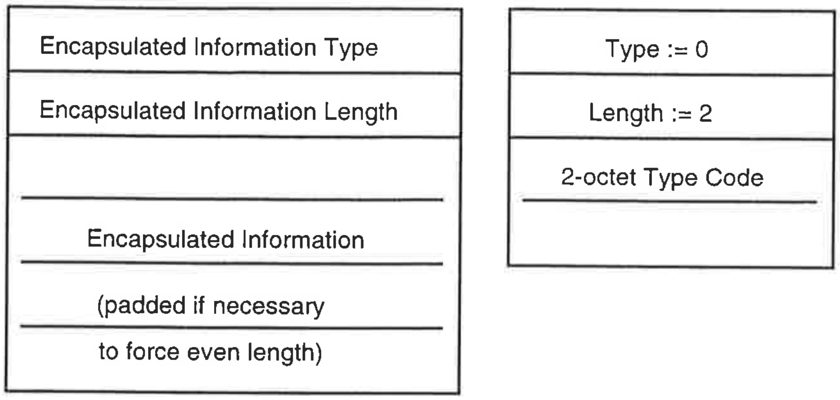

Figure 1. Encapsulated Information Element Format and Values for Type 2 Ethernet

The encapsulated information element plus the basic MSDU payload must fit within the 2304–octet maximum MSDU payload size. This is not expected to be a problem, because 1500 octets is the largest MSDU payload from any of the instances of ill–behaved, non–802 LANs identified to date.

Rules for Using Encapsulated Information Elements

1. A portal which integrates an ill–behaved, non–802 LAN (a LAN that puts LLC–visible information in its MAC header) shall generate an encapsulated information element to hold this information as a part of the MSDU payload of each frame distributed within the ESS after receipt from the integrated LAN. The resulting MSDUs shall be sent using data subtypes in the range 8–15. When such a portal receives a frame containing an encapsulated information element from within the ESS, the encapsulated information shall be used to generate the appropriate field(s) of the integrated LAN frame, as indicated by the type of the encapsulated information element.

2. A portal which integrates a conventional, 802–type LAN shall discard encapsulated information elements on MSDUs received from the within the ESS unless there is a generally–accepted method of handling the particular type of ancillary information indicated by the encapsulated information element type over the 802–type LAN integrated by this portal.

3. All stations of an ESS involved in the inter–station transfer of frames for distribution services (e.g. APs and stations that are part of a WDS) shall forward all MSDUs as appropriate for their addressing information, leaving any encapsulated information elements intact.

4. All other stations, upon valid reception of an MSDU containing an encapsulated information element, may either discard the encapsulated information, or may report that information to the local LLC entity as status information, not as part of the MSDU payload. (The suggested manner of reporting is to use the "reception_status" parameter of the MA–UNITDATA.indication.) These stations are not required to be able to generate encapsulated information elements; however, these stations may generate MSDUs with encapsulated information elements if their implementation provides a means for the LLC entity to request such generation and to provide the information to be encapsulated.