IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Recommendations to REVme on ESS | | | | |
| Date: 2021-07-16 | | | | |
| Author: | | | | |
| Name | Affiliation | Address | Phone | Email |
| Mark Hamilton | Ruckus/CommScope | 350 W. Java Dr,  Sunnyvale, CA | +1.303.818.8472 | [mark.hamilton2152@gmail.com](mailto:mark.hamilton2152@gmail.com) |

##### This is a set of recommendations from 802.11’s ARC SC to 802.11’s REVme, for modification of Draft Standard text on the definition and introductory discussion of the concepts “ESS” and “HESS”.

##### Revision history:

##### R0 – Initial draft

##### R1 – Updated during review by ARC SC at 802.11 F2F, January 2020, Irvine, CA, USA

##### R2 – Updated references to be against REVmd D4.0 (was D3.0). (Only change is the reference to subclause 11.22.2.)

##### R3 – Per REVmd telecon on Sep 14, 2020: Now a personal contribution, with the following changes:

* Minor changes to 4.3.5.2 proposed text (highlighted in yellow).
* Explicitly listed the additional locations to change “homogeneous ESS” (checking for various spellings) with “HeSS”. (Changes highlighted in yellow.)
* Added discussion of how the contents of 4.3.20 and 4.5.9 could be further updated in this general direction, and why that is suggested to be deferred, for now.

R4 – From off-line comments, two minor editorial changes, marked in blue.

R5 – Removed historical changes tracking (highlights, etc., that are described above). Added references to Wi-Fi Alliance specs, and discussion of potential additions to connect the HeSS concepts to the Wi-Fi Alliance uses, as examples. Minor editorial changes, per ARC SC call on Jan 11, 2021.

R6 – Added NOTE to 11.22.2 to clarify the orthogonality of HeSS and SSID. Per Joe Levy email of Jan 13, 2021, added some changes to clarify that GLK operation is separate from, and how it differs from, ESS and DS operation.

R7 – Updated introduction letter. Per review in ARC SC telecon of Feb 1, 2021, resolved/agreed a few additional changes on HeSS, and added some new topics to the “deferred topics” list, for further study within ARC.

R8 – Editorial changes to address to REVme instead of REVmd.

R9 – Editorial cleanup in preparation for presentation in REVme.

R10 – Editorial corrections suggested on July 15 telecon. Added some new future considerations identified on the call, in the Deferred topics section.

**Recommendations from ARC SC to REVme**

Mike, et al,

Some time ago (approx. May 2016), during joint discussions between ARC SC, TGak, and 802.1, the question was asked “What [really] is an ESS?” The ARC SC has been researching and debating this question as a background task ever since, and has finally reached some conclusions/recommendations.

From our review, we recommend the following changes, to be considered by REVme. While these changes appear to be a significant re-definition of a very fundamental concept to IEEE Std 802.11, we believe that the changes are, conceptually, really not that different – it is a matter of using correct terminology and being consistent with terms and usage elsewhere in the Standard, and with most experts’ conceptual model of an ESS. Hence, we believe these changes are appropriate, and request REVme’s consideration.

An earlier version of this document (r4) was presented to REVmd, in September 2020. This latest version of these recommendations is the result of some follow-on discussion and refinement around the HeSS concepts.

If the task group is interested in deeper background and history of this discussion, our working document can be found here: <https://mentor.ieee.org/802.11/dcn/18/11-18-1051-13-0arc-what-is-an-ess.pptx>

Thank you for your time and consideration.

Mark Hamilton, Chair ARC SC

--

All references are to REVmd D5.0.

**Modify the definition of ESS (in clause 3):**

* + - From:

“A set of one or more interconnected basic service sets (BSSs) that appears as a single BSS to the logical link control (LLC) layer at any station (STA) associated with one of those BSSs.”

* + - To:

“A set of one or more basic service sets (BSSs) that are interconnected by a single distribution system (DS); an ESS appears as a single IEEE Std 802™ access domain to the logical link control (LLC) sublayer.”

**Modify text in 4.3.5.1 (the “Overview” subclause of the “DS concepts” subclause):**

* + - From:

“The DS enables mobile device support by providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.

An access point (AP) is any entity that has STA functionality and a distribution system access function (DSAF), which enables access to the DS, via the WM for associated STAs.”

* + - To:

“The DS enables mobile device support by providing the logical services necessary to handle address to destination mapping and seamless integration of multiple BSSs.

An access point (AP) is any entity that has STA functionality and a distribution system access function (DSAF), which enables access to the DS, via the WM for associated STAs. To access the DS, a non-AP STA joins a BSS and associates with the AP operating that BSS. This causes the AP to notify the DS of the non-AP STA’s location within the network. The non-AP STA moves to another BSS operated by an AP connected to the same DS in another location by reassociating with this new AP. The new AP updates the DS with the non-AP STA’s new location at the completion of the reassociation.

The STA’s location information is internal to the DS, thus STA mobility is transparent to upper layers. See 4.3.5.2 (Extended service set (ESS): the large coverage network).”

**Modify text in 4.3.5.2 (“Extended service set (ESS): the large coverage network”):**

* + - From:

“The DS and infrastructure BSSs allow IEEE Std 802.11 to create a wireless network of arbitrary size and complexity. IEEE Std 802.11 refers to this type of network as the ESS. An ESS is the union of the infrastructure BSSs with the same SSID connected by a DS. The ESS does not include the DS.

The key concept is that the ESS appears the same to an LLC layer as an IBSS. STAs within an ESS can communicate and mobile STAs might move from one BSS to another (within the same ESS) transparently to LLC.”

* + - To:

“The DS and infrastructure BSSs allow IEEE Std 802.11 to create a wireless network of arbitrary size and complexity. IEEE Std 802.11 refers to this type of network as the ESS. An ESS is the union of the infrastructure BSSs with the same SSID connected by a single DS. All BSSs in an ESS have the same SSID. The ESS does not include the DS.

The key concept is that the ESS appears to be a single IEEE Std 802™ access domain to the LLC sublayer ~~the same to an LLC layer as an IBSS~~. STAs within an ESS can communicate and mobile STAs might move from one BSS to another (within the same ESS) transparently to the LLC sublayer.

If multiple BSSs are configured with the same SSID, but the APs are not interconnected by a common DS, there is no guarantee of seamless mobility for STAs between those BSSs. However, such a deployment may have a common LLC sublayer interconnection, in which case, communication with location transparency to the LLC sublayer (a single access domain) is generally still possible, but such communication could be disrupted at times when a mobile STA moves between BSSs.”

**Replace the definition of “homogeneous extended service set (ESS)” (in clause 3):**

**Change from:**

* + “homogeneous extended service set (ESS): A collection of basic service sets (BSSs), which may or may not be within the same extended service set (ESS), in which every subscription service provider network (SSPN) or other external network reachable at one BSS is reachable at all of them”

**To (and put in alphabetical order):**

* + “HeSS: A collection of basic service sets (BSSs) that provide access to a set of higher-layer services using a given set of authentication credentials
  + NOTE1—HeSS is an orthogonal concept to extended service set (ESS). Membership of a given BSS in an HeSS is independent of any ESS membership.
  + NOTE2—“HeSS” is not an abbreviation for anything.

**And update the abbreviation:**

**Change from:**

* HESSID (#1352)homogeneous extended service set identifier

**To:**

* HESSID HeSS identifier

**In 9.4.2.91 (Interworking element) change:**

The HESSID field, which is the identifier for a homogeneous ESS, specifies the value of HESSID; …

**to**

The HESSID field, which is the identifier for an HeSS, specifies the value of HESSID; …

**In the HESS discussion text (in 11.22.2):**

**Replace:**

* + In an infrastructure BSS, the Interworking element contains signaling for Homogeneous ESSs. The HESSID is a 6-octet MAC address that identifies the homogeneous ESS. The HESSID value shall be identical to one of the BSSIDs in the homogeneous ESS. Thus, it is a globally unique identifier that, in conjunction with the SSID, may be used to provide network identification for an SSPN.
  + NOTE—This standard assumes that the HESSID field in the Interworking element is administered consistently across all BSSs in a homogeneous ESS.

**With:**

* + In an infrastructure BSS, the Interworking element contains signaling for HeSSs. The HESSID is a 6-octet MAC address that identifies the HeSS. The HESSID value shall be identical to one of the BSSIDs in the HeSS. The HESSID is a globally unique identifier that identifies a set of higher-layer services and the authentication credentials required to access them.
  + NOTE—This standard assumes that the HESSID field in the Interworking element is administered consistently across all BSSs in an HeSS.
  + NOTE—The concept of an HeSS is orthogonal to an ESS, and any SSIDs can be used by the BSSs that provide access to the HeSS. For more information on HeSS, refer to Wi-Fi Alliance documents [Bx] and [By].

**In the MIB, change (in the DESCRIPTION of dot11HESSID):**

This attribute is used by an AP and is the 6-octet homogeneous ESS identifier field, whose value is set to one of the BSSIDs in the ESS. It is required that the same value of HESSID be used for all BSSs in the homogeneous ESS.

**to:**

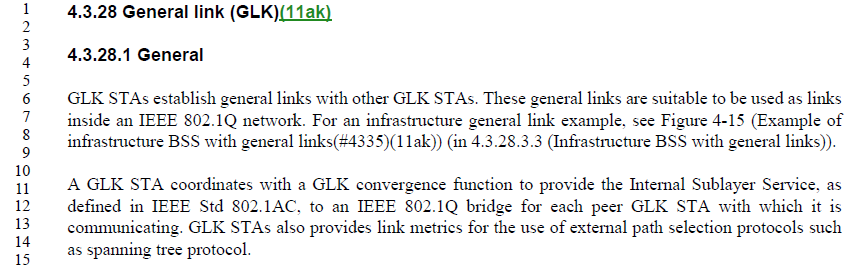
This attribute is used by an AP and is the 6-octet HeSS identifier field, whose value is set to one of the BSSIDs in the HeSS. It is required that the same value of HESSID be used for all BSSs in the HeSS."

**Add two informative references to the Annex A Bibliography:**

[Bx] Wi-Fi Alliance Passpoint Specification, Version 3.2

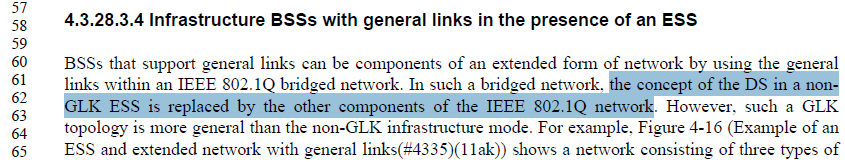
[By] Wi-Fi Alliance, Wi-Fi CERTIFIED Passpoint Deployment Guidelines Rev 1.3

**In 4.3.28.1, add a new paragraph after the second paragraph:**

****

Add: “GLK operation does not involve a DS and does not involve an ESS. Instead, the general links formed with GLK operation are a point-to-point connection between pairs of instances of Internal Sublayer Service SAPs, which in turn can be used within an IEEE 802.1Q bridged network.”

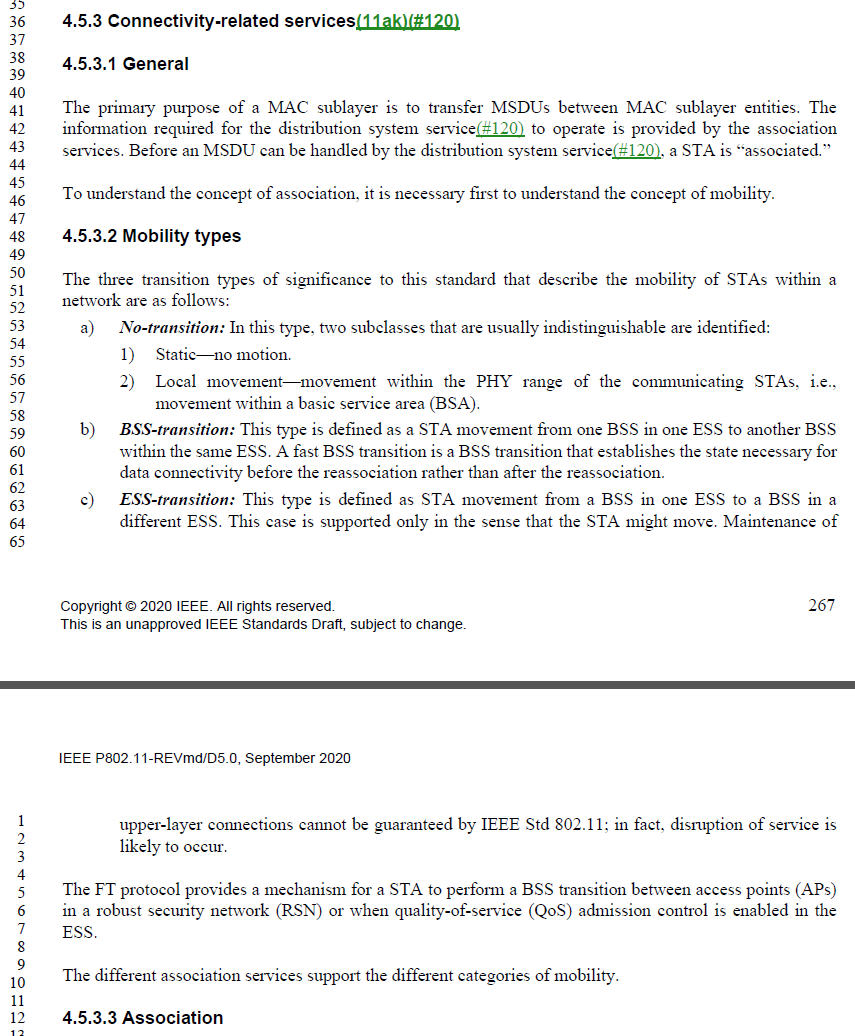
**In 4.3.28.3.4** it states: “… the concept of the DS in a non-GLK ESS is replaced by the other components of the IEEE 802.1Q network.) (260.61) **Delete “non-GLK” (and change “a” to “an”).**



**In 4.5.3.2 mobility types are defined – the types defined apply to non-GLK, but there is no discussion of GLK mobility types or which of the defined types apply to GLK.**

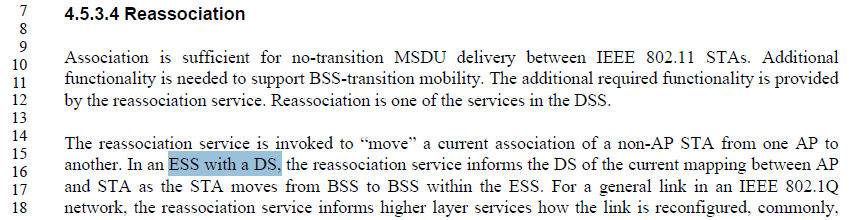
**Note in clause 4.5.3.4 (269.17) there is a description of mobility for GLK.**

In 4.5.3.2, first paragraph, change “mobility of STAs” to “mobility of non-GLK STAs”. In the last paragraph, change “different categories of mobility” to “different categories of non-GLK mobility”. Add a new last paragraph, as below:



“In GLK operation, association services establish a general link between a pair of instances of Internal Sublayer Service SAPs. For these links there is no DS to provide the distribution service. Association services coordinate with higher layer services to create and maintain an IEEE 802.1Q network. Mobility of GLK links is managed (if supported at all) by the ability of the associated IEEE 802.1Q bridged network and the associated GLK convergence function (shim layer) to support remapping a general link from one IEEE 802.1Q bridge port to another. Such operation is outside the scope of IEEE 802.11, but see 4.5.3.4 for some concepts used for GLK link mobility.

**In 4.5.3.4 replace “ESS with a DS” to simply be “ESS”:**



**Deferred changes/potential future work:**

The following are other topics that ARC SC identified during discussion of the above changes. 802.11 members may want to consider this further work. ARC SC welcomes TGme’s input on whether to take on this work, and if so in which group.

**Subclause 4.3.20 is “Subscription service provider network (SSPN) interface”.**

There are two paragraphs in this subclause and one Figure (Figure 4-8) which are meant to help describe the concept of an SSPN. It mentions concepts such as how the SSPN and AP exchange authentication information (outside the scope of this standard). It also describes that the SSPN interface (a logical ‘link’ between the SSPN and the non-AP STA) “provides the non-AP STA with access to the services provisioned in the SSPN.”

Deeper review of these paragraphs may result in some suggestions from Interworking experts to help connect the concept of HeSS into these paragraphs. There is currently no mention of the HeSS concept in this subclause.

There is a reference to “ESS” in Figure 4-8, which is arguably possible/allowed, but not really relevant to the subclause’s concepts. This could be changed to “HeSS”, perhaps. We should coordinate that with overall review/update of this subclause in conjunction with Interworking experts.

**Subclause 4.5.9 is “Interworking with external networks”.**

This subclause is more extensive than 4.3.20. Topics are focused around the general concepts of Interworking, including PAD, and other services. This subclause also has mention of the SSPN interface and access to SSPN, and might also benefit from some more explanation of how HeSS fits into the concepts.

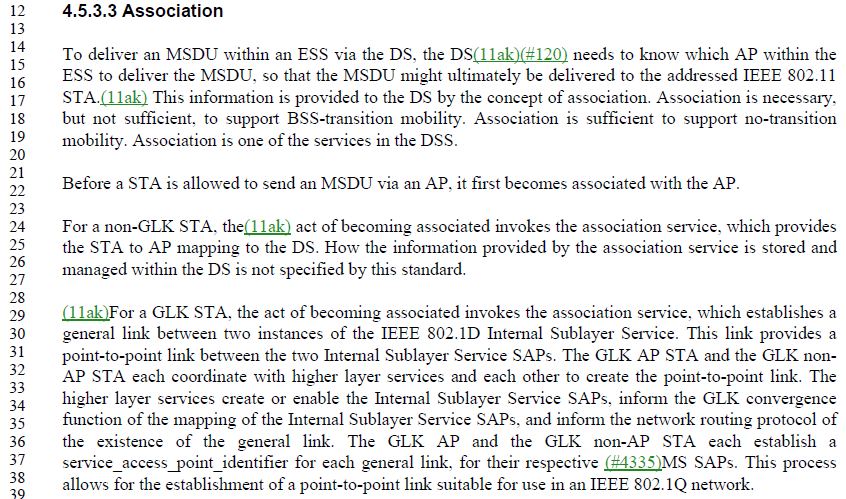
There is currently no discussion of the HeSS concept in this subclause.

There is a reference to “ESS” in subclause 4.5.9.2.4 (Service information registry), which might be correctly HeSS. This should also be discussed with Interworking experts, as part of any expansion/correction of subclause 4.5.9.

**Do we also suggest adding clarifications on ANQP usage (behavior across all APs in an HeSS should be the same (for some ANQP, but not all), etc.)?**

**General cleanup of GLK operation’s use of [Re][Dis]Association:**

3c) 4.5.3.3 Association seems to have a minor problem that it states: “Association is one of the services in the DSS.” (268.19) While this is a true statement it makes no mention of association for GLK which is described later in the section (268.29) and seems to me to not allow for association with out a DSS, which is not true as association is allowed with in a BSS and does not require an ESS. [Replace: “Association is one of the services in the DSS.” With: “Maintaining a list of APs and their associated STAs is one of the services in the DSS.”]



3d) 4.5.3.4 Reassociation also has the same minor problem that it states: “Reassociation is one of the services in the DSS.“ [Replace: “Reassociation is one of the services in the DSS” With: “Maintaining a list of APs and their associated STAs is one of the services in the DSS.”]

3f) 4.5.3.5 Disassociation also has the same minor problem that it states: “Disassociation is one of the services in the DSS.” [Replace: “Disassociation is one of the services in the DSS” With: “Maintaining a list of APs and their associated STAs is one of the services in the DSS.”]

Proposed Change: Insert “In non-GLK operation,” before “Association is one of the services in the DSS.” Same thing in 4.5.3.4.

Move to the Deferred topics – perhaps expand into an overall cleanup of GLK operation w.r.t. association/etc (“GLK association”?)

**Is there anything we want to address regarding “ESS Link” as part of the ESS definition fix?**

For further discussion. - Move to the Deferred topics – perhaps “BSS link” is a concept. Are the uses really ESS-specific, necessarily, or general BSS link uses? Also, need to fix the definition (of ESS link) to be between a non-AP STA and \_the associated\_ AP (which is an “ESS AP”).

**There are some interesting uses of ESS in clause 12 which may need review. e.g., can a STA be a member of an ESS and can a STA associate with an ESS.**

For further discussion. - Move to the Deferred topics

**A STA associates with a DS? (or an ESS?) or with an AP?**

For further discussion. - Move to the Deferred topics

**Terminology: A STA [re]associates “to” or “with” an AP?**

For further discussion. - Move to the Deferred topics

**Is there a DoS attack, due to the DS updating its mapping table “at the completion of [re]association”, but in an RSN the 4-way handshake has not completed and the requesting device is not (may not be?) authenticated, yet.**

For further discussion. - Move to the Deferred topics