IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Proposed Comment Resolutions for NSEP Priority Access (CC34) | | | | |
| Date: 2021-03-xx | | | | |
| Author(s): | | | | |
| Name | Company | Address | Phone | email |
| Subir Das  John Wullert  Kiran Rege | Perspecta Labs |  |  | (sdas,jwullert, krege) @perspectalabs.com |
| An Nguyen ,  Frank Suraci | DHS/CISA/ECD |  |  | (an.p.nguyen, frank.suraci) @cisa.dhs.gov |
| Dibakar Das | Intel |  |  | Dibakar.das@intel.com |
| Chittabrata Ghosh | Facebook |  |  | Chittabrata@fb.com |
| Leif Wilhelmsson | Ericsson |  |  | leif.r.wilhelmsson@ericsson.com |
| Matthew Fischer | Broadcom |  |  | matthew.fischer@BROADCOM.COM |
| Gaurav Patwardhan | Hewlett Packard Enterprise (HPE) |  |  | gaurav.patwardhan@hpe.com |
| Sam Sambasivan | AT&T |  |  | Sam\_Sambasivan@labs.att.com |

Abstract

This document proposes comment resolutions for the following CIDs (12) on NSEP Priority Access from the 80.11be D0.3 comment collection 34 (CC34):

1110, 1112, 1721, 1722, 1820, 2257, 2258, 2264, 2265, 2266, 2274, 3345

Revisions:

- Rev 0: Initial version of the document.

Interpretation of a Motion to Adopt

A motion to approve this submission means that the editing instructions and any changed or added material are actioned in the TGbe Draft. This introduction is not part of the adopted material.

**Editing instructions formatted like this are intended to be copied into the TGbe Draft (i.e. they are instructions to the 802.11 editor on how to merge the text with the baseline documents).**

**TGbe Editor: Editing instructions preceded by “TGbe Editor” are instructions to the TGbe editor to modify existing material in the TGbe draft. As a result of adopting the changes, the TGbe editor will execute the instructions rather than copy them to the TGbe Draft.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Commenter** | **Clause Number** | **Page/**  **Line** | **Comment** | **Proposed Change** | **Resolution** |
| 2264 | Michael Montemurro | 4.5.11a | 35.1 | The text describing AP behavior is cumbersome for a Clause 4 description. | change: "APs that have NSEP priority access activated advertise this capability in Beacon and Probe Response frames. Non-AP STAs that intend to use NSEP priority access query APs that advertise NSEP priority access to gain additional details prior to association. During association, APs verify the authority of non-AP STAs to use NSEP priority access. This could be accomplished using a subscription service provider's authorization infrastructure via an SSPN interface. The AP might store the results of this authorization process locally to enable subsequent verification. AP might also use this information to confirm authority during (re)association." to "APs advertise this capability and authorize Non-AP STAs to use NSEP priority access. APs authorize non-AP STAs to use NSEP priority access based on locally available information or through a service provider's authorization infrastructure via an SSPN interface. The AP might cache results the authorization information locally to enable subsequent verification and use it to confirm authority during (re)association." | **Revised:**  **Editor: Please replace the first paragraph (lines 1-8), page 35 in Clause 4.5. 11a with the following:**  “AP MLDs or EHT APs that have NSEP priority access activated advertise this capability and authorize Non-AP MLDs or non-AP EHT STAs to use NSEP priority access. AP-MLDs or EHT APs authorize non-AP MLDs or non-AP EHT STA to use NSEP priority access based on locally available information or through a service provider's authorization infrastructure via an SSPN interface. The AP-MLD or EHT AP might cache authorization information locally to enable subsequent verification and use it to confirm authority during (re)association.” |
| 1110 | Alfred Asterjadhi | 4.5.11a | 35.1 | Activation is different from capable. An AP may be capable but not activated the service yet. Suggest to clarify here. | As in comment. | **Revised and addressed by CID #2264** |
| 1112 | Alfred Asterjadhi | 4.5.11a | 35.23 | Seems odd to use another request to disable NSEP priority access. Suggest referring to a teardown frame. Similar consideration in the normative behavior subclause. | As in comment. | **Revised:**  **Editor: Please replace the text in line 22/23, page 35 in Clause 4.5.11a “Either the AP or the non-AP STA can disable NSEP priority access by sending another request.” with the following :**  Either the AP MLD or EHT AP or the non-AP MLD or non-AP EHT STA can disable NSEP priority access. |
| 1721 | Hanseul Hong | 4.5.11a | 35.1 | The main description of negotiation process and corresponding operation is described in Clause 35.10. Specify if the AP and non-AP STA are EHT AP and EHT non-AP STA | As in the comment | **Revised.**  **Editor: Changes are made in all NSEP clauses. Once the suggested changes are accepted, no additional action is required for this comment.** |
| 1722 | Hanseul Hong | 4.5.11a | 35.22 | The detailed operation will be included in Clause 35.10.3. Add the referece for 'preferential treatment' | Add 'as described in 35.10.3 (NSEP priority access procedure)' after 'preferential treatment' | **Accepted.**  **Editor: Please add the proposed text at the end of line 22, page 35 in Clause 4.5.11a:** |
| 1820 | James Yee | 4.5.11a | 35.22 | "preferential treatment" is ambiguous and should be replaced with a more accurate description. | As suggested | **Revised.**  **Editor: Please replace the term “preferential treatment “ in line 22, Clause 4.5.11a with the following:**  treating NSEP traffic with a higher priority. |
| 2257 | Michael Montemurro | 3.1 | 29.9 | The definition could be improved. This term describes access, not traffic. | Replace "On-demand capability that provides higher priority to traffic generated by authorized non-access point (AP) stations(STA) and to ﾠtraffic destined for authorized non-AP STAs." with "An on-demand capability that allows an access point (AP) to authorize a non-access point (AP) stations (STA) to communicate National Security and Emergency Preparedness (NSEP) traffic." | **Revised:**  **Editor: Please replace the NSEP definition (lines 9-12), page 29 in Clause 3.1 with the following:**  An on-demand capability that allows access points multi-link devices (AP MLDs) or EHT APs to authorize non-access point multi-link devices (non-AP MLDs) or non-AP EHT stations (STA) to communicate National Security and Emergency Preparedness (NSEP) traffic with a higher priority. |
| 3345 | Zhiqiang Han | 3.1 | 29.10 | This definition conflicts with the following one(NSEP Traffic). Based on the definition of NSEP traffic, it's better to change "and" to "or". | as the comment | **Revised and addressed by CID #2257** |
| 2258 | Michael Montemurro | 3.1 | 29.15 | Change enabled to authorized | Change "enabled" to "authorized" | **Revised:**  **Editor: Please update the NSEP traffic definition (lines 14-15), page 29 in Clause 3.1 with the following:**  The traffic generated by a non-access point multi-link device (MLD) or non-AP EHT STA or traffic destined for a non-AP MLD or non-AP EHT STA when the NSEP priority access is authorized and enabled. |
| 2265 | Michael Montemurro | 4.5.11a | 35.11 | The note is not required and the text can be clearer. | Change: "NSEP priority access operates in an on-demand fashion. The STA invokes NSEP priority access when instructed to do so by an authorized user or a managed service provider who detects the need for priority. NOTE 1--Detecting the need for priority is outside the scope of this standard." to "A STA invokes NSEP priority access on-demand when instructed to do so by an authorized user or a managed service provider who detects the need for priority. Detecting the need for NSEP priority access for a STA is outside the scope of this standard." | **Revised:**  **Editor: Please replace lines 11-14, page 35, Clause 4.5.11a with the following:**  An MLD or an EHT STA invokes NSEP priority access on-demand when instructed to do so by a higher layer function, such as an authorized user or a managed service provider who detects the need for priority. Detecting the need for NSEP priority access for an MLD or an EHT STA is outside the scope of this standard. |
| 2266 | Michael Montemurro | 4.5.11a | 35.16 | This text is cumbersome and could be improved. It is not consistent with other clause 4 text. | Replace "The non-AP STA requests NSEP priority access by sending a request to the AP. The AP confirms the authority of the non-AP STA to use NSEP priority access, e.g., using the locally stored verification information or reaching out to NSEP service provider via the SSPN interface, and sends a response to the requesting non-AP STA. Alternatively, the AP can enable NSEP priority access by sending an unsolicited request to a non-AP STA, and the non-AP STA confirms the request by sending a response. While NSEP priority access is enabled, all traffic to and from the non-AP is provided with preferential treatment. Either the AP or the non-AP STA can disable NSEP priority access by sending another request. NOTE 2--The means by which the AP determines the need for priority is outside the scope of this standard." with "Non-AP STAs enable NSEP priority access by sending a request to an AP that advertises the capability. The AP authorizes the non-AP STA using locally stored verification information or information received from an NSEP service provider via the SSPN interface and sends a response to the non-AP STA. Alternatively, the AP can enable NSEP priority access by sending an unsolicited request to an authorized non-AP STA, and the non-AP STA confirms the request by sending a response.  While NSEP priority access is enabled, all traffic to and from the non-AP is provided with NSEP priority access treatment. Either the AP or the non-AP STA can disable NSEP priority access by a request to terminate priority access." | **Revised.**  **Editor: Please replace lines 16-25 in page 35, Clause 4.5.11a with the following:**  Non-AP MLDs or non-AP EHT STAs enable NSEP priority access by sending a request to an AP-MLD or an EHT AP that advertises the capability. The AP MLD or EHT AP authorizes the non-AP MLD or non-AP EHT STA using locally stored verification information or information received from an NSEP service provider via the SSPN interface and sends a response to the non-AP MLD or non-AP EHT STA. Alternatively, the AP MLD or EHT AP can enable NSEP priority access by sending an unsolicited request to a non-AP MLD or a non-AP EHT STA and the non-AP MLD or non EHT STA confirms the request by sending a response.  While NSEP priority access is enabled, all traffic to and from the non-AP MLD or non-AP EHT STA is treated with a higher priority, as described in 35.10.3 (NSEP priority access procedure). Either the AP MLD or EHT AP or the non-AP MLD or non-AP EHT STA can disable NSEP priority access. |
| 2274 | Michael Montemurro | 11 | 87.1 | NSEP looks like an interworking procedure (at least that's how its described in clause 4. There should be at least a cross reference within interworking that references the specification text in clause 35 | Update clause 11.22.5 with at least a reference to clause 35. | **Rejected:**  Reason is that changes associated with EHT are described in clause 35 and Clause 35.10.1 does refer to Clause 11.22.5. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 2460 | Payam Torab Jahromi | Draft P802.11be\_D0.3.pdf |  | NSEP priority access is PHY independent; for broader reach and impact on installed base detach the definition from EHT. | MAC | **Rejected.**  No idea which clause/page number the comment is referred to. |

**\*\*\*\* Editor: Please update the following Clauses as revised below: \*\*\*\***

**3. Definitions, acronyms, and abbreviations**

**3.1 Definitions**

**National Security and Emergency Preparedness (NSEP) priority access**: ~~On-demand capability that provides higher priority to traffic generated by authorized non-access point (AP) stations (STA) and to traffic destined for authorized non-AP STAs.~~ An on-demand capability that allows ~~access points (APs)~~ access point (AP) multi-link devices (MLDs) or enhanced high throughput (EHT) access point (AP) to authorize non-access point (non-AP) MLDs, or non-AP STAs ~~stations (STA)~~ to communicate National Security and Emergency Preparedness (NSEP) traffic with a higher priority. [#2257 #3345]

**National Security and Emergency Preparedness (NSEP) traffic**: The traffic generated by a non-access point (non-AP) multi-link device (MLD) or a non-AP enhanced high throughput station (EHT STA) ~~station (STA)~~ or traffic destined for a ~~non-AP~~ non-AP MLD or a non-AP EHT ~~station (STA)~~ when the NSEP priority access is authorized and [#2258 ] enabled.

**4.5.11a NSEP priority access**

Existing national security and emergency preparedness (NSEP) communications services[[1]](#footnote-1) in multiple countries provide priority for voice and data exchanges on public networks. NSEP priority access is intended to provide capabilities to support such priority services on IEEE 802.11-based networks[[2]](#footnote-2).

NSEP priority access provides prioritized access to system resources for authorized users to increase their probability of successful communication during periods of network congestion. Priority access involves treating the NSEP traffic with a higher priority, as described in 35.10.3 (NSEP priority access procedure), [ #1722 and #1820] in obtaining channel access and in allocation of network resources. The service is only available to designated, authorized devices who normally represent a small fraction of the overall number of devices operating in the area.

~~APs that have NSEP priority access activated advertise this capability in Beacon and Probe Response frames. Non-AP STAs that intend to use NSEP priority access query APs that advertise NSEP priority access to gain additional details prior to association. During association, APs verify the authority of non-AP STAs to use NSEP priority access. This could be accomplished using a subscription service provider’s authorization infrastructure via an SSPN interface. The AP might store the results of this authorization process locally to enable subsequent verification. AP might also use this information to confirm authority during (re)association.~~

AP MLDs or EHT APs that have NSEP priority access activated advertise their support for, and verify the authority of Non-AP MLDs or non-AP EHT STAs to use, NSEP priority access. AP MLDs authorize non-AP MLDs or non-AP STAs to use NSEP priority access based on locally available information or through a service provider's authorization infrastructure via an SSPN interface. The AP MLD or EHT AP might cache authorization information locally to enable subsequent verification and use it to confirm authority during (re)association. [#1110, #2264]

~~NSEP priority access operates in an on-demand fashion. The STA invokes NSEP priority access when instructed to do so by an authorized user or a managed service provider who detects the need for priority.~~

~~NOTE 1—Detecting the need for priority is outside the scope of this standard~~.

An MLD or an EHT STA invokes NSEP priority access on-demand when instructed to do so by a higher layer function, such as an authorized user or a managed service provider who detects the need for priority. Detecting the need for NSEP priority access for an MLD or a STA is outside the scope of this standard. [#2265]

~~The non-AP STA requests NSEP priority access by sending a request to the AP. The AP confirms the authority of the non-AP STA to use NSEP priority access, e.g., using the locally stored verification information or reaching out to NSEP service provider via the SSPN interface, and sends a response to the requesting non-AP STA. Alternatively, the AP can enable NSEP priority access by sending an unsolicited request to a non-AP STA, and the non-AP STA confirms the request by sending a response. While NSEP priority access is enabled, all traffic to and from the non-AP is provided with preferential treatment. Either the AP or the non-AP STA can disable NSEP priority access by sending another request.~~

~~NOTE 2—The means by which the AP determines the need for priority is outside the scope of this standard.~~

Non-AP MLDs or non-AP EHT STAs enable NSEP priority access by sending a request to an associated AP MLD or an EHT AP that advertises the capability. The non-AP MLD can send the request on any available link between the non-AP MLD and the AP MLD. The AP MLD or the EHT AP authorizes the non-AP MLD or non-AP EHT STA using locally stored verification information or information received from an NSEP service provider via the SSPN interface and sends a response to the non-AP MLD or non-AP EHT STA. Alternatively, the AP MLD or EHT AP can enable NSEP priority access by sending an unsolicited request to a non-AP MLD or non-AP EHT STA and the non-AP MLD or non-AP EHT STA confirms the request by sending a response.

While NSEP priority access is enabled, all traffic to and from the non-AP MLD or non-AP EHT STA is treated with a higher priority, as described in 35.10.3 (NSEP priority access procedure). Either the AP MLD or EHT AP or the non-AP MLD or non-AP STA can disable NSEP priority access. [#1112, #2266]

1. For example, NSEP Services in the United States, including the Government Emergency Telecommunications Service and the Wireless Priority Service, run on commercial operator networks and are managed by the Emergency Communications Division of the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security. [↑](#footnote-ref-1)
2. Priority access capabilities to support these services in other types of networks are defined in appropriate international standards, (e.g., Multimedia Priority Service (MPS) in 3GPP). [↑](#footnote-ref-2)