IEEE P802.11
Wireless LANs

|  |
| --- |
| Unsupported Opclasses in RNR and FILS-FD |
| Date: 2023-9-1 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Thomas Derham | Broadcom | San Diego, CA, USA |  | thomas.derham@broadcom.com |

Abstract

An issue has been identified that could result in interoperability issues when a legacy non-AP STA attempts to discover and connect to a 320 MHz EHT AP, due to differing interpretations of the standard with regard to the selection of the Operating Class advertised in Reduced Neighbor Report. A somewhat similar issue potentially also exists with FILS Discovery frames.

The issues are described and proposed text to resolve them is proposed.

R1 – some text revised for clarity based on offline feedback. Approach for FILS-DF made consistent with approach proposed for RNR.

R2 – remove the minor (and probably out-of-scope) editorial fix to baseline text in the paragraph starting “When the reporting AP cannot…” in 11.49; this will also help avoid any conflicts with CID 6325 from TGme SA ballot on that paragraph. Note: the author also confirmed there are no other current CIDs in TGme on the subclauses modified by this submission.

**Discussion on RNR:**

The Reduced Neighbor Report (RNR) element is an important part of out-of-band discovery, particularly discovery of 6 GHz BSSs.

RNR is broadcast by APs in Beacon and Probe Response frames of a (reporting) BSS, and advertises the existence of neighboring (reported) BSSs that are often operating on a different band.

The Operating Class and Channel Number fields in a Neighbor AP Information field in RNR are intended to indicate channel information for the neighboring BSS(s) indicated in that Neighbor AP Information field. Non-AP STAs receive RNR and typically use this channel information to efficiently and selectively scan (6 GHz) channels to discover those BSS(s).

Subclause 9.4.2.169 currently defines these two fields as follows:

* “Operating Class field indicates a channel starting frequency that, together with the Channel Number field, indicates the primary channel of the BSSs…”
* “Channel Number field indicates the last primary channel of the APs…. Channel Number is defined within an Operating Class as shown in Table E-4…”

In addition, subclause 11.49 currently states the following:

* “The Operating Class field is selected from values in Table E-4 filtered by the requirement that, together with the Channel Number field, the primary channel be identifiable. NOTE 2 – For instance, this excludes operating class 128-130”

Note that, with respect to Table E-4, operating classes 128-130 (as referenced in the note above) are for 5 GHz 80, 160 and 80+80 channel spacing in 5 GHz band and, unlike 5 GHz operating classes 115 thru 127, are not associated with a channel set that identifies a primary channel (instead, they are associated with channel center frequency indices). Therefore it is fairly clear from this text (although certainly subject to misinterpretation) that the specified operating class is expected to be one that is associated with a channel set of primary channels.

Unfortunately, current implementations (with RNR support) in the field have mostly (or possibly universally) taken an approach that is not exactly aligned with that interpretation. Instead, AP implementations are setting the Operating Class field to the operating class with channel spacing equal to the BSS bandwidth.

For example, when AP implementations advertise a reported 6 GHz BSS with 160 MHz bandwidth and primary channel 37 in RNR, they set the Operating Class field to 133 and the Channel Number field to 37. Then, the non-AP STA implementation determines the actual primary channel frequency using the Channel Number field and the Channel Starting Frequency associated with the operating class in the Operating Class field. Note that operating class 133 corresponds to channel spacing of 160 MHz, however channel number 37 is a member of the channel set for operating class 131 (whereas operating class 133 only specifies a set of channel center frequency indices).

The 11be draft introduces a new operating class with 320 MHz channel spacing in 6 GHz band (operating class 137). This value will not in general be understood by existing 6 GHz non-AP STAs in the field; however those STAs are still expected to discover 320 MHz BSSs using RNR (and, for example, connect using HE PHY/MAC on the primary 160 of the BSS).

If 11be AP implementations were to continue to follow that approach (i.e. setting the Operating Class field to 137), it is likely to cause interoperability issues for existing non-AP STAs since the Channel Number field alone does not in general uniquely identify the actual primary channel. For example, primary channel number 149 in 6 GHz (operating class 131; channel starting frequency 5.950 GHz) is also a valid primary channel number in 5 GHz (operating class 125; channel starting frequency 5 GHz).

Since the list of valid Operating Classes in Table E-4 is regularly expanded in various amendments and maintenance projects in accordance with new capabilities (e.g. wider bandwidths) and changes in regulations in various countries, a generic approach is needed to avoid similar issues in the future.

Therefore, the proposed resolution modifies the current definitions of these fields with three objectives:

* To be compatible with the approach taken by most/all existing implementation in the field, and
* To be compatible with the approach currently defined in 802.11, and
* To avoid interoperability issues where some operating class(es) supported by an AP are not known by (part of) the cohort of non-AP STAs that are able to connect to that AP.

***TGbe editor: Add the following text to 11be draft 4.0*:**

**9.4.2.170 Reduced Neighbor Report element**

**9.4.2.170.2 Neighbor AP Information field**

***Change NOTE 1 as follows:***

NOTE 1—The Operating Class field and Channel Number tuple indicate the primary channel in order to assist with passive scanning. Selection of the operating class is defined in subclause 11.49 (Reduced neighbor report).

* Reduced neighbor report

***TGbe editor: Add the following text at the start of subclause 11.49 to 11be draft 4.0:***

***Change the 7th and 8th paragraphs (including to split and extend the 7th paragraph) as follows:***

The Reduced Neighbor Report element contains a list of operating classes and primary channels along with TBTT information for the reported neighbor APs or colocated APs on each operating class and primary channel.

The primary channel is a value from the Channel set column of Table E-4 (Global operating classes) that indicates the primary channel of the reported APs in the Neighbor AP Information field.

The operating class is one of the ~~selected from~~ values in Table E-4 (Global operating classes) ~~filtered by the requirement that, together with the Channel Number field, the primary channel be identifiable.~~ for which all the following are true:

* The operating class has the same Channel starting frequency as the primary channel, and
* The operating class’s Channel set or Channel center frequency index set contain a channel that fully encompasses the primary channel, and
* The operating class’s channel spacing is equal to or less than the BSS bandwidth of all the reported APs in the Neighbor AP Information field

If there are multiple operating classes in Table E-4 for which all the above are true, the AP should select (one of) the operating class(es) that is expected to be understood by all STAs that might intend to connect to the reported AP, even if the channel spacing of that operating class is less than the BSS bandwidth of all the reported APs in the Neighbor AP Information field.

NOTE 2 – STAs conformant with an earlier revision of this standard might not understand all the operating classes defined in Table E-4 (Global operating classes). The above recommendation is intended to maximize backward compatibility. For example, if an AP reports an EHT AP that is operating a BSS with 320 MHz bandwidth in 6 GHz band using operating class 137, it is recommended that the operating class selected by the AP in the Reduced Neighbor Report element is operating class 131, 132, 133 or 134, since these are expected to be understood by all STAs that can connect to the reported 6 GHz AP.

The center frequency of the primary channel is determined from the Channel starting frequency identified by the Operating Class field, together with the Channel Number field.

~~NOTE 2—For instance, this excludes operating class 128–130.~~

## End of change

**Discussion on FILS Discovery frames (and other frames/elements):**

The duple of <Operating Class> and <Channel Number> (or some variant thereof) is also used in various other frames and elements.

In cases where those frames/elements are sent unicast, this is not necessarily a problem because (presumably) the transmitter is expected to indicate an Operating Class value that will be understood by the receiver. The basis on which the transmitter makes such determination is not necessarily clear, but in principle could be based on the list specifies in Supported Operating Classes element sent in (Re)Association Requests (by STA) or in Beacons / Probe Responses (by APs). It is possible some notes/guidance could be useful in this regard, but they are not proposed in this document.

However, one other case where the duple is *broadcast* is in FILS Discovery frames sent in non-HT Dup format. Recent efforts in REVme have clarified the definition of these fields; it is explicitly stated that the channel spacing of the specified operating class must equal the BSS bandwidth. Therefore, in principle this could result in a similar interoperability issue as discussed for RNR, if the specified operating class is unknown by the receiving non-AP STA. Theoretically, this issue might be mitigated by the fact that (unlike RNR), the channel starting frequency of the specified primary channel is always equal to the channel starting frequency of the channel on which the (FILS Discovery) frame is received. Since the receiving STA knows the channel number number on which it received the frame, it could theoretically determine the actual primary channel using the value in the Primary Channel subfield alone. However, given there are existing implementations in the field that do not handle that case, similar changes as for RNR are proposed as follows:

* FILS Discovery frame format

***TGbe editor: Add the following text at the end of subclause 9.6.7.36 in 11be draft 4.0*:**

***Modify paragraphs 29 and 30 as follows:***

The Operating Class and Primary Channel subfields are present if the FILS Discovery frame is transmitted in a non-HT duplicate PPDU. Otherwise, the subfields are not present. Selection of the operating class is defined in subclause 11.45.2.1 (FILS Discovery frame transmission).

When present, the subfields indicate the following:

* If the operating class has a channel spacing other than 80 MHz
* A minimum possible value for the BSS bandwidth, i.e. the BSS bandwidth is greater than or equal~~s~~ to the channel spacing
* Center frequency of the primary XX MHz channel ~~on which the BSS operates~~, where XX is the channel spacing
* Center frequency of the primary channel

NOTE XXX: If the channel spacing is equal to the BSS bandwidth, then the center frequency of the primary XX MHz channel is equal to the center frequency of the channel on which the BSS operates

* If the operating class has a channel spacing of 80 MHz
* A minimum possible value for the BSS bandwidth, i.e. the BSS bandwidth is greater than or equal to ~~either~~ 80 MHz, or equal to 80+80 MHz
* Center frequency of the primary 80 MHz channel~~, if BSS bandwidth is 80+80 MHz~~
* Center frequency of the primary channel

## End of change

***TGbe editor: Add the following text as subclause 11.45.2.1 in 11be draft 4.0*:**

﻿**11.45 Fast Initial Link Setup (FILS) procedures**

**﻿11.45.2 FILS Discovery frame generation and usage**

**11.45.2.1 FILS Discovery frame transmission**

***Modify paragraph 2 as follows, and renumber existing notes 1 and 2 as notes 2 and 3:***

﻿An AP may transmit a FILS Discovery frame as a non-HT duplicate PPDU. When a FILS Discovery frame is transmitted as a non-HT duplicate PPDU, its operating class and primary channel shall be indicated by its Operating Class and Primary Channel fields, respectively. The operating class is one of the values in Table E-4 (Global operating classes) for which all the following are true:

* The operating class has the same Channel starting frequency as the primary channel, and
* The operating class’s Channel set or Channel center frequency index set contain a channel that fully encompasses the primary channel, and
* The operating class’s channel spacing is equal to or less than the BSS bandwidth of the AP

If there are multiple operating classes in Table E-4 for which all the above are true, the AP should select (one of) the operating class(es) that is expected to be understood by all STAs that might intend to connect to the AP, even if the channel spacing of that operating class is less than the BSS bandwidth of the AP.

NOTE 1 – STAs conformant with an earlier revision of this standard might not understand all the operating classes defined in Table E-4 (Global operating classes). The above recommendation is intended to maximize backward compatibility. For example, if an AP that is operating a BSS with 320 MHz bandwidth in 6 GHz band using operating class 137, and is transmitting FILS Discovery frames in Non-HT Dup format, it is recommended that the AP indicates operating class 131, 132, 133 or 134 in this frame, since these are expected to be understood by all STAs that can connect to the AP.

## End of change