802.11bi Draft Specification

|  |
| --- |
| Proposed spec texts for probe request |
| Date: 2023-06-28 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com |
| Ido Ouzieli |  |  |  |
| Robert Stacey |  |  |  |
| Daniel F Bravo |  |  |  |
| Danny Alexander |  |  |  |

Abstract

This submission proposes spec text based on the following passed requirement.

*11bi shall define a minimal set of Elements for transmission by a CPE Client in a probe request**prior to authentication.*

*11bi shall define a mechanism for the 11bi non-AP STA to refrain from transmitting Probe Request frames containing elements except TBD element(s)*

Revision History:

* Rev 0: Initial version of the document

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

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

Discussion:

11be has the following rules with the motivation of minimizing the size of Probe Request frame.

* + - 1. ***Probe Request frame content for a non-AP EHT STA***

*An EHT AP shall follow the rules defined in 11.1.4.3.4 (Criteria for sending a response) when receiving a Probe Request frame addressed to it even if the frame does not contain some of the elements described in Table 9-66 (Probe Request frame body) when the soliciting non-AP STA follows the rules described in this subclause.*

*If a non-AP EHT STA is sending a Probe Request frame that is not an multi-link probe request:*

* *it shall follow the rules defined in 9.3.3.9 (Probe Request frame format) regarding the inclusion of the SSID element, the Supported Rates and BSS Membership Selectors field, the Request element, the Extended Supported Rates and BSS Membership Selectors element, the DSSS Parameter Set element, the SSID List element, the Extended Request element, the FILS Request Parameters element, the Short SSID List element, Vendor Specific elements, and the Known BSSID element,*
* *it may omit other elements listed in 9.3.3.9 (Probe Request frame format) and may disregard the normative requirements in 9.3.3.9 (Probe Request frame format) for these other elements.*

*If a non-AP EHT STA is sending (#16188)a multi-link probe request:*

* *it shall follow the rules defined in 9.3.3.9 (Probe Request frame format) regarding the inclusion of the SSID element, the Supported Rates and BSS Membership Selectors field, the Extended Supported Rates and BSS Membership Selectors element, and the DSSS Parameter Set element,*
* *it shall follow the rules defined in* [*35.3.4.2 (Use of multi-link probe request and response)*](#_bookmark22) *regarding the inclusion of the Request element, the Extended Request element, and the Probe Request Multi- Link element,*
* *it shall not include the other elements listed in 9.3.3.9 (Probe Request frame format) and shall disregard the normative requirements in 9.3.3.9 (Probe Request frame format) for these other elements.*

For the elements that are still listed in the paragraph of Probe Request frame,

* The The privacy concern for the SSID element is already addressed by the following baseline spec texts in 12.2.10 Requirements for support of MAC privacy enhancements.
	+ *To avoid leakage of possibly sensitive network identifying information, STAs should refrain from transmitting Probe Request frames containing preferred SSID values and, instead, use passive scanning or transmit Probe Request frames containing the wildcard SSID.*
* The DSSS Parameter Set element is only required in 2.4 GHz when dot11RadioMeasurementActivated is true, if needed, the client can switch dot11RadioMeasurementActivated to off before sending Probe Request. Even if the DSSS parameter Set element is sent, it is usually just primary channel, which is likely the channel used to transmit DSSS parameter set anyway
	+ *The DSSS Parameter Set element is present within Probe Request frames generated by STAs using Clause 15 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), Clause 16 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), or Clause 18 (Extended Rate PHY (ERP) specification) PHYs if dot11RadioMeasurementActivated is true.The DSSS Parameter Set element is present within Probe Request frames generated by STAs using a Clause 19 (High Throughput (HT) PHY specification(#2297)) PHY in the 2.4 GHz band if dot11RadioMeasurementActivated is true.*
	+ *A STA that transmits a frame that contains both an HT Operation element and a DSSS Parameter Set element shall set the Primary Channel field in the HT Operation element to the same value as the Current Channel field in the DSSS Parameter Set element.*
* The Request element is already optionally present in Table 9-66—Probe Request frame body and client can omit it to have privacy



* The SSID List element is already optionally present in Table 9-66—Probe Request frame body and the privacy issue is addressed by the sentence in 12.2.10



* The Extened Reqeust element is already optionally present in Table 9-66—Probe Request frame body and client can omit it to have privacy



* The FILS Request Parameters element is already optionally present in Table 9-66—Probe Request frame body and client can omit it to have privacy



* The Short SSID List element is already optionally present in Table 9-66—Probe Request frame body and the privacy issue is addressed by the sentence in 12.2.10



* The Vendor Specific element is already optionally present in Table 9-66—Probe Request frame body and client can omit it to have privacy



* The Known BSSID element is already optionally present in Table 9-66—Probe Request frame body and client can omit it to have privacy



Multi-link probe request can be replaced by the protected action frame to request capabilities and operation parameters.

The remaining elements that are still worthwhile for discussions are the Supported Rates and BSS Membership Selectors element and the Extended Supported Rates and BSS Membership Selectors element, which are also listed as the target for entropy fingerprinting in “Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms”.



These fields are useful in 11.1.4.6 (Operation of Supported Rates and BSS Membership Selectors element and Extended Supported Rates and BSS Membership Selectors element) for AP to indicate the required rate to join the BSS and for client to indicate the rate that can be used for reception.

For client, the only relevant information in probe request is the OperationalRateSet becasues client only gets BSSBasicRateSet parameter and the BSS membership selectors after discovery.

*A STA shall include the rates from its OperationalRateSet parameter and the rates from the BSSBasicRateSet parameter and the BSS membership selectors from the BSSMembershipSelectorSet parameter in frames it transmits containing Supported Rates and BSS Membership Selectors elements and Extended Supported Rates and BSS Membership Selectors elements according to the rules described in this subclause with the following exceptions:(#24)*

*1) A non-AP STA may omit the HT and VHT BSS membership selectors, as the (V)HT capabilities are indicated through the presence of a (V)HT Capabilities element.*

*2) An S1G or CMMG STA should not include supported rates in frames it transmits since its*

*MCS capabilities are indicated in its Capabilities element. An S1G or CMMG STA should*

*ignore supported rates in frames it receives since the peer’s MCS capabilities are indicated in*

*its Capabilities element*

*Upon receipt, the Supported Rates and BSS Membership Selectors element in Beacon and Probe Response frames is delivered to the management entity in a STA via the BSSBasicRateSet parameter in the MLME-SCAN.confirm primitive. The BSS membership selector information in Beacon and Probe Response frames is delivered to the management entity in a STA via the BSSMembershipSelectorSet parameter in the MLME-SCAN.confirm primitive. Together, these parameters are used by the management entity in a STA to avoid joining(#1465) a BSS if the STA cannot receive and transmit all of the data rates in the BSSBasicRateSet parameter or does not support all of the features represented in the BSSMembershipSelectorSet parameter.*

We propose that the 11bi client just indicates the mandatory rate up to 11n. As a result, every 11bi device indicates the same value in Supported Rates and BSS Membership Selectors element and there are no privacy issues.

***19.1.1 Introduction to the HT PHY***

*In addition to the requirements found in Clause 19 (High Throughput (HT) PHY specification(#2297)), an HT STA shall support(#546) transmitting and receiving frames that are compliant with the mandatory PHY specifications defined as follows:*

*— In Clause 17 (Orthogonal frequency division multiplexing (OFDM) PHY specification) when the*

*HT STA is operating in a 20 MHz channel width in the 5 GHz band*

*— In Clause 16 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification) and*

*Clause 18 (Extended Rate PHY (ERP) specification) when the HT STA is operating in a 20 MHz channel width in the 2.4 GHz band*

***17.1.1 General***

*This clause specifies the PHY entity for an orthogonal frequency division multiplexing (OFDM) system. The OFDM system provides a WLAN with data payload communication capabilities of 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s. The support of transmitting and receiving at data rates of 6, 12, and 24 Mb/s is mandatory. The system uses 52 subcarriers that are modulated using binary or quadrature phase shift keying (BPSK or QPSK) or using 16- or 64-quadrature amplitude modulation (16-QAM or 64-QAM). Forward error correction coding (convolutional coding) is used with a coding rate of 1/2, 2/3, or 3/4.*

***18.1.2 Introduction***

*The ERP builds on the payload data rates of 1 and 2 Mb/s, as described in Clause 15 (DSSS PHY specification for the 2.4 GHz band designated for ISM applications), that use DSSS modulation and builds on the payload data rates of 1, 2, 5.5, and 11 Mb/s, as described in Clause 16 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification), that use DSSS and CCK. An ERP STA shall comply with all normative requirements of Clause 16 (High rate direct sequence spread spectrum (HR/DSSS) PHY specification). The ERP draws from Clause 17 (Orthogonal frequency division multiplexing (OFDM) PHY specification) to provide additional payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mb/s. Of these rates, transmission and reception capability for 1, 2, 5.5, 6, 11, 12, and 24 Mb/s data rates is mandatory*

**Proposed Texts:**

**TGbi Editor: *Instruction: Insert 12.13.x Contents of Probe Request frame as shown below***

**12.13 Client Privacy Enhancement**

**12.13.x Contents of Probe Request frame**

This subclause defines rules for the contents of a Probe Request frame that is not a multi-link probe request to preserve privacy.

An EDP STA follows the rules defined in 35.3.4.5 (Probe Request frame content for a non-AP EHT STA) to determine the contents of a Probe Request frame that is not a multi-link probe request with the following exception:

* In 2.4 GHz, the EDP STA should indicate only 1, 2, 5.5, 6, 11, 12, and 24 Mb/s in the Supported Rates and BSS Membership Selectors element and should not include the Extended Supported Rates and BSS Membership Selectors element
* In 5 GHz or 6 GHz, the EDP STA should indicate only 6, 12, and 24 Mb/s in the Supported Rates and BSS Membership Selectors element and should not include the Extended Supported Rates and BSS Membership Selectors element

NOTE – The inclusion of the Request element, the SSID List element, the Extended Request element, the FILS Request Parameters element, the Short SSID List element, Vendor Specific elements, and the Known BSSID element is optional as described in Table 9-66—Probe Request frame body and an EDP STA can choose not to include these elements to preserve privacy.

NOTE – The EDP STA can follow the rule defined in 12.2.10 (Requirements for support of MAC privacy enhancements) to avoid leakage of possibly sensitive network identifying information in SSID element.