Interpretation #1

Interpretation Number: 1-05/03 (status codes)
Topic: 802.11 status codes
Relevant Clauses: 7.3.1.9
Classification: unambiguous

Interpretation Request

In clause 7 there are several status codes defined that appear in several different frames. Yet, when each of these status codes is to be transmitted and any action to be taken by a station upon reception of these status codes is not specified. Please specify the use of the status codes on both transmission and reception.

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003)

The standard defines as valid a set of status codes for use in management frames defined in clause 7 and in MLME primitives defined in clause 10. Normative behavior is provided for status code 0, corresponding to successful status code. Transmission of some status codes during authentication, association and re-association processes are described in Annex C. The standard does not define normative behavior for transmitting other status codes. Reception of status codes is defined by the standard in that the code is passed across the MLME SAP interface to an external entity outside the scope of the standard. This item is being brought to the attention of the 802.11 working group for the possibility of action in a future revision or maintenance change.

Interpretation #2

Interpretation Number: 2-05/03 (status codes)
Topic: 802.11 reason codes
Relevant Clauses: 7.3.1.7
Classification: unambiguous

Interpretation Request

In clause 7 of IEEE Std. 802.11-1999, the content of a Reason Code field is defined that appears in several different 802.11 frames. There is not any definition of the use of each of the different reason codes on transmission nor any definition of the behavior of a station upon reception of these reason codes. Please define the use of these reason codes for both transmission and reception.

Interpretation for IEEE std 802.11-1999 (reaffirmed 2003)

The standard defines as valid a set of reason codes for use in management frames defined in clause 7 and in MLME SAP primitives defined in clause 10. Transmission of some reason codes during authentication, association and re-association processes are described in Annex C. The standard does not define normative behavior for transmitting other reason codes. Reception of reason codes is defined by the standard in that the code is passed across the MLME SAP interface to an external entity outside the scope of the standard. This item is being brought to the attention of the 802.11 working group for the possibility of action in a future revision or maintenance change.

Interpretation #3

Interpretation Number: 3-05/03 (802.11a channels) Topic: 802.11a channel definitions Relevant Clauses: 17.3.8.3.1, 17.3.8.3.2, 17.3.8.3 Classification: unambiguous
Interpretation Request
In IEEE Std. 802.11a-1999, 200 channels are defined, one each centered every 5 MHz from 5000 MHZ to 6000 MHz. Yet only 12 of these channels are defined as legal and only in the US-NII radio bands. How are legal channels defined for regulatory domains, other than the US?
Interpretation for IEEE std 802.11-1999 (reaffirmed 2003)
The standard defines as valid a set of only those channels for use in the US U-NII band. See clause 17.3.8.3.3 for this definition. It does not define how other sets of valid channels are defined. Current work in both 802.11h and 802.11j are addressing this issue. This item is being brought to the attention of the 802.11 working group for the possibility of action in a future revision or maintenance change.

Interpretation #4

Interpretation Number: 4-05/03 (Country Information Element)
Topic: Country Information Element Relevant
Clauses: 7.3.2.9 (7.3.2.12 from the requester), 17.3.8.3.3
Classification: unambiguous

Interpretation Request

Abstract
The current description of the country information element is vague about the precise contents

of the country information element. It remains unclear whether the country information must always contain the full set of regulatory domain information as specified by the regulatory administrations or that a subset of the regulatory domain information can be used as specified by the network operator. Furthermore, it is ambiguous how the country information element should be used in the 5GHz band.

Current definition of the country information element
The country information element contains the information required to allow a station to identify the regulatory domain in which the station is located and to configure its PHY for operation in that regulatory domain.

Vague rules for sub band definition in 2GHz band
The country information element allows the definition of multiple sub bands with each their own maximum transmit power levels.

The rules specified for these sub bands are:

- sub band ranges must not overlap;
- sub bands must monotonically increase.

This definition does not demand that sub bands exactly fill up the regulatory channels.

For example, this definition allows network operators to create a country element as follows:
The country element contains three sub bands.
1) The First Channel Number element of the first sub band is set to channel 1 and the Number of Channels element is set to one.
2) The First Channel Number element of the second sub band is set to channel 5 and the Number of Channels element is set to one.
3) The First Channel Number element of the third sub band is set tot channel 9 and the Number of Channels element is set to one.

The resulting country information element is valid within the FCC regulatory domain and might be valid to the definition of the country information element in the IEEE 802.11d standard.

STAs that use the above country information to determine the regulatory domain, will only mark channels 1, 5 and 9 as regulatory permitted and will not look for networks at the other channels. Although this may improve the scanning behavior of STAs, we believe this is not what the country information element is intended for according to the definition in the first paragraph of section 7.3.2.12 (lines 30-32 of page 1 of this document).

Proposal
Change text to clearly state that the country information element must be used to inform STAs about the full regulatory domain of operation. Sub bands may only be used if the regulatory domain consists of sub bands.

Proposed text change
(802.11d, page 4, paragraph 4): Change “The group of channels described .. increasing in channel numbers.” into “The group of channels described by each pair of the First Channel Number and Number of Channels fields shall not overlap, shall be monotonically increasing in channel numbers and shall describe all channels allowed in the regulatory domain.”

Interpretation for IEEE std 802.11-1999 (reaffirmed 2003)
The definition of the use of the Country information element in either of the cases described by the requester is allowed in the standard. The Country information element provides a mechanism to communicate information relevant to the configuration of a radio necessary for proper operation in a regulatory domain. The standard does not limit the use of this mechanism to transfer only information identical to that required for the full use of bands (or sub-bands) defined for the regulatory domain.

It is possible that some clarifying text might be helpful to guide the implementer to the expect either of these uses of the mechanism. This is being brought to the attention of the 802.11 working group with the possibility of action in a future revision or maintenance change.

Interpretation Request

Ambiguous definition in 5GHz band
It is not defined how to use the country information element in the 5GHz band. Unlike the 2GHz band, in the 5GHz band channels numbers specify the center frequencies of 20MHz wide channels. Channel numbers below 240 are encoded as steps of 5MHz from the 5GHz base (e.g. channel 36 => 5GHz + (36*0.005) = 5.18GHz). Channel numbers from 240 and up are defined as negative channel numbers with steps of 5MHz from base 5GHz (e.g. channel 240 = 5GHz – (16*0.005) = 4.92GHz).

Channels in the 5GHz band are always spaced 20MHz apart. If the channel number of a channel is 40, its neighboring channels will have channel numbers 36 and 44 respectively.

The ambiguity in the country information element is the definition of a sub band in the 5GHz. If the channel number is set to 36 and the number of channels is set to 4, does this imply that this sub band consists of channels 36, 40, 44 and 48 or consists of channels 36, 37, 38 and 39? The latter definition would not make any sense with respect to the 20MHz wide channels.

Proposal
Add text to describe that the channel number specifies the first channel of the sub band and

that in the 5GHz band the number of channels specifies the number of 20MHz wide channels in the sub band.

Proposed text addition
(802.11d, page 4, paragraph 5): Add following text after: “The Number of Channels field .. in length.” “In the 5GHz band, it shall contain a positive integer value that indicates the number of 20MHz wide channels in the sub band adjacent to the first channel. Expressed in channel numbers this implies that the last channel in the sub band will have channel number First Channel Number + ((Number of Channels –1) * 4).”

Interpretation for IEEE std 802.11-1999 (reaffirmed 2003)

Because the channel numbers are specific to a particular PHY, it is critical to understanding how the channel number and number of channels is used in the Country information element to refer to the definition of valid, or legal, channels defined in the PHY. For the instance cited by the requester, the 5 GHz PHY defines those valid channels in clause 17.3.8.3.3. For a First Channel Number of 36 and a Number of Channels of 4 in a Country information element the individual channel numbers defined for the 5 GHz PHY by these parameters are 36, 40, 44, and 48.

It is possible that some clarifying text might be helpful to guide the implementer to the information already in the standard. This is being brought to the attention of the 802.11 working group with the possibility of action in a future revision or maintenance change.

Interpretation #5

Interpretation Number: 1-07/03 (delayed CFP Beacon)
Topic: 802.11 Beacon
Relevant Clauses: 9.3.3.2
Classification: unambiguous

Interpretation Request

original line : In the case of a busy medium due to DCF traffic, the beacon shall be delayed for the time required to complete the current DCF frame exchange.

I think there is no direct answer about the following case.

Q : When a PCF beacon(CFPeriod=0, DTIM COunt=0) is defered due to a busy medium(DCF), PC shall use xxxxxxxxxx delay to start the CFP after this DCF medium busy.

A :
<1> served as normal DCF beacon, use DIFS+random backoff delay
<2> served as normal PCF beacon while not deffered by medium, use PIFS delay

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003)

Clause 9.3.3.2 says, in part: "… the PC shall use a DIFS plus a random backoff delay (with CW in the range of 1 to aCWmin) to start a CFP when the initial beacon is delayed because of deferral due to a busy medium." This is a clear statement that the Beacon is to be transmitted using a backoff after DIFS after the medium becomes idle.

This area of the standard is being modified by the work going on 802.11 Task Group e. You may be interested in following that work as it progresses.

Interpretation #6

Interpretation Number: 1-09/03 (Contention window and retry counters)
Topic: Reset of contention window to CWmin
Relevant Clauses: 9.2.4, 9.2.5.3
Classification: unambiguous

Interpretation Request

According to the above sub-clauses, the Station {Short, Long} Retry counters are incremented every time a (Short/Long) retry counter associated with an MSDU is incremented. They are only reset upon successful transmission of an MPDU (of appropriate length).

The CW is 'controlled' by the Station counters, increasing in size every time either of the Station counters increases. It is reset to CWmin only
a) after a successful MSDU transmission, or
b) when either of the Station counters reaches their respective limit.

Consider a scenario where a station *continually* fails to transmit successfully: The CW will increase, until condition b) above is met, at which point it will revert to CWmin. However, the Station retry counters are not reset at this point, and will continue to increase; condition b) will not be met again, and CW will increase (or remain at CWmax) for all subsequent (failed) attempts, regardless of the state of the respective MSDU counters.

Is this the intended behavior? It seems odd that the CW will be reset after the first failure (when b) is met, and the MSDU is discarded), but not for subsequent MSDUs.

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003)

The requester's interpretation of the standard is correct. The standard allows the contention window to be reset to CWmin in this situation only once, after which the CW value will progress to the largest value in the sequence and remain there until one of the conditions to reset the CW to CWmin is met. This behavior is intended to minimize the bandwidth wasted by a station that is unable to successfully exchange frames with its intended receiver(s).

Interpretation #7

Interpretation Number: 2-09/03 (Maximum transmit power level in Country information element)
Topic: Maximum transmit power level in Country information element
Relevant Clauses: 7.3.2.9
Classification: unambiguous

Interpretation Request (part 1)

The phrase "…maximum power…allowed to be transmitted" is ambiguous.
The most likely interpretations include:

1. TPO (Transmitter Power Output)
2. EIRP (Effective Isotropically Radiated Power)

Unfortunately, different administrations have regulations that are based on either TPO (e.g. FCC) or EIRP (e.g. ETSI), and in such a way that they cannot always be converted into one another. E.g. the FCC specifies a maximum TPO and allows up to 6dBi antenna gain. Above 6dBi the TPO should be reduced dB for dB, except for point-to-point links, where a higher antenna gain is allowed and less reduction is to be applied. This cannot be converted to an equivalent EIRP limit. ETSI specifies a plain EIRP limit.

What is the interpretation of the Maximum Transmit Power Level field?

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003) (part 1)

The interpretation of a value in the Maximum Transmit Power Level field of a Country information element does not need be expressed as TPO, EIRP, or any other particular means of measurement. The interpretation is defined by the regulations of the country identified in the

Country String of the same information element. Assuming the examples provided by the requester are correct, this would mean that a value in the Maximum Transmit Power Level field of a Country information element with a Country String value of “US” would be interpreted as a measure of the TPO of the device, whereas a value in an information element where the value of the Country String is “NL” would be interpreted as a masue of the EIRP of the device.

Interpretation Request (part 2)

Apart from a limit on radiated power, the regulations usually contain a PSD (Power Spectral Density) limit. In some domains, the PSD limit is more strict than the TPO/EIRP limit and thus further limits the transmitted power.

Example: The EIRP limit under ETSI regulations in the 5150-5350 MHz band is 200mW, but the PSD limit is 10mW/MHz EIRP. Since an OFDM signal has a bandwidth of 16MHz, the EIRP is further limited to approximately 160mW.

Should, in this case, the Maximum Transmit Power Level field be set to 200mW or 160mW?

If the interpretation is plain EIRP, the station will exceed PSD limits for certain countries, since the PSD limit is not part of the country information elements. How should in that case the PSD limit be derived?

If the interpretation is to take the PSD limit into account in the Maximum Transmit Power Level, we have to integrate the PSD over the signal bandwidth to convert to total power. However, there is a problem in the 2.4GHz band, since the spectral shape for DSSS/CCK is not accurately defined, so that the conversion factor may depend on the transmitter filter implementation (and thus may vary for each client STA). What conversion factor should be used in that case?

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003) (part 2)

The information in the Country information element provides an indication of the regulatory domain and the requirements of that domain. It is not expected that the information in the information element is sufficient to configure all of the parameters of a device to comply with the regulations in effect in the regulatory domain. The value of the Maximum Transmit Power Level is to contain the value specified in the regulations of the particular regulatory domain identified by the value of the Country String. It is up to each manufacturer to use the information in the Country information element, along with local configuration information, such as a power backoff value, to configure a device for operation that is compliant with the local regulations where the device is operating.

Interpretation Request (part 3)

The Country Information Element does not indicate whether a particular subband has indoor/outdoor restrictions. How should this information be derived?

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003) (part 3)

The Country information element provides, as part of the Country String, an indication as to whether the bands described in the information element are utilizing regulations that are differentiated for indoor and outdoor operation. While an access point or station may be sending a Beacon or Probe Response containing a Country information element that does not match the location of the receiver, i.e., an access point that is indoors might be received outdoors, it is expected that the receiver will utilize the information in the Country String and determine its local configuration based on that information. There is no mechanism specified in the standard to convey both indoor and outdoor information for a single band or to describe one or more subbands for indoor operation and one or more other subbands for outdoor operation.

Interpretation #8

Interpretation Number: 1-01/04 (Use of Status and Reason Codes)
Topic: Usage of Status and Reason Codes
Relevant Clauses: 7.3.1.7, 7.3.1.9
Classification: unambiguous

Interpretation Request

Values for the Reason Code are defined in clause 7.3.1.7 and values for the Status Code are defined in clause 7.3.1.9. These values are to be included in various MAC Management frames. However, there is no definition of when a station or AP is to transmit a particular value for these items, nor what a station or AP is to do upon receipt of a particular value for these items.
\

How are the values for the Reason Code and Status Code to be selected for transmission and what is to be done upon reception of each code?

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003)

This request duplicates requests that have been received in the past. The response to these requests is available on the IEEE 802.11 web site at the following URLs:

http://www.ieee802.org/11/Interpretations/03-402r1-M-Interpretation_Response_02-0503.doc
http://www.ieee802.org/11/Interpretations/03-401r1-M-Interpretation_Response_01-0503.doc

This information has been forwarded to the 802.11 working group for consideration of inclusion in a future revision or maintenance release of the standard.

Interpretation #9

Interpretation Number: 2-01/04 (Undefined information elements)
Topic: Definition of certain information elements
Relevant Clauses: 7.3.2
Classification: unambiguous

Interpretation Request

In 2002, the 802.11 Working Group created a set of Element IDs, defining the use of many information elements defined as "Reserved" in the standard. Many of these element IDs are assigned for the use of individual companies. An additional element ID is defined as a "vendor-specific" information element. The format and use of these newly defined information elements is not described in the standard or any of its supplements.

What is the format of each of the information elements defined by the newly assigned element IDs, when are they used, and in which frames may they appear?

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003)

The standard defines the information element IDs that are the subject of the interpretation request as “reserved”. This includes the working group-assigned information element IDs for the use of individual companies and the “vendor-specific” information element. This indicates that the element IDs may be used in a future amendment of the standard. The standard does not provide any definition of the use of these information element IDs for individual company use or for use as a “vendor-specific” information element. The request has been forwarded to the 802.11 working group for consideration of inclusion in a future revision or maintenance release of the standard.

Interpretation #10

Interpretation Number: 1-03/04 (Adopting beacon parameters in an IBSS)
Topic: Adopting beacon parameters in an IBSS
Relevant Clauses: 3.8, 7.2.3, 7.3.2.2, 9.1.2, 10.3.3.1, 10.3.2.2, 11.1.2.2, 11.1.3, 11.1.4

Classification: ambiguous

Interpretation Request

11.1.4 says: “A STA receiving such a frame [a beacon] from another STA in an IBSS with the same SSID shall compare the Timestamp field with its own TSF time. If the Timestamp field of the received frame is later than its own TSF time, the STA shall adopt all parameters contained in the Beacon frame.”

What is the meaning of “all parameters” in this context? It’s clearly not just the TSF timer, or there would be no need to say “all” parameters. And if it includes information carried in IEs, does it, or does it not, include IEs which the STA does not recognize?

Interpretation for IEEE STD 802.11-1999 (reaffirmed 2003)

The items in question are identified in clause 10.3.3.1 (MLME-JOIN.request), which in turns references the enumerated list within BSSDescription in clause 10.3.2.2 (MLME-SCAN.confirm).

Each BSSDescription consists of the following elements:

- BSSID – A STA in IBSS mode receiving this field in a beacon would adopt this value since this is the identification value for the IBSS assigned per clause 11.1.3.
- SSID – A STA in IBSS mode receiving this field in a beacon would adopt this value, as stated explicitly in clause 11.1.4.
- BSSType – A STA in IBSS mode receiving this field in a beacon would implicitly adopt this value, because the STA is operating in IBSS mode.
- Beacon Period – A STA in IBSS mode receiving this field in a beacon would adopt this value, as stated explicitly in clause 11.1.2.2.
- DTIM Period – A STA in IBSS mode receiving this field in a beacon would adopt this value, as stated explicitly in clause 11.1.2.2.
- Timestamp – A STA in IBSS mode receiving this field in a beacon would adopt this value, as stated explicitly in clause 11.1.4.
- Local time – This field is not applicable to this interpretation request since this is a local value used for computational purposes in adopting the TSF of the peer MAC entity (per clause 11.1.4) and is not a beacon parameter per se.
- PHY parameter set – A STA in IBSS mode receiving this field in a beacon would adopt this value.
- CF parameter set – A STA in IBSS mode receiving this field in a beacon would not adopt this value since a CFP is not allowed in an IBSS (per clause 9.1.2).
- IBSS parameter set – A STA in IBSS mode receiving this field in a beacon would adopt this value.
- Capability Information – A STA in IBSS mode receiving this field in a beacon would not adopt this value since this value in the local MAC entity must represent the advertised capabilities of the local MAC entity.
- BSSBasicRateSet – Per clause 3.8, “the BSS basic rate set data rates are preset for all

stations in the BSS". A STA participating in a BSS is required to "avoid associating with a BSS if the STA cannot receive and transmit all the data rates in the BSS basic rate set" per clause 7.3.2.2.

Processing of unknown IEs is defined in clause 7.2.3.

This information has been forwarded to the 802.11 working group for consideration of inclusion in a future revision or maintenance release of the standard.

Interpretation #11

Interpretation Number: 2-03/04 (Reinitializing the 802.11b scrambler for header and psdu fields)
Topic: Reinitializing the 802.11b scrambler for header and psdu fields
Relevant Clauses: 15.2.3, 15.2.4
Classification: unambiguous

Interpretation Request

I have doubt regarding scrambling in 802.11b. For each packet we have 3 fields (plcp header, plcp preamble and psdu). while scrambling plcp preamble we are initializing with particular seed based on preamble. What about header and psdu fields. We have to be reinitialize the scrambler state or not?

Interpretation for IEEE STD 802.11b-1999 (reaffirmed 2003)

IEEE STD 802.11b-1999 (reaffirmed 2003) clearly states the requirements for scrambling in clauses 15.2.3 and 15.2.4. Since the standard is clear on this matter, no interpretation is required.

Interpretation #12

Interpretation Number: 1-11/04 (Annex G acccuracy)
Topic: Accuracy of material in Annex G
Relevant Clauses: Annex G
Classification: Conflicts with clause 17

Interpretation Request

A possible mistake was found while working with IEEE 802.11a standard, as follows:

1. Designation of the standard, including the year of publication.

IEEE Std 802.11a-1999
Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications
High-speed Physical Layer in the 5 GHz Band

2. The specific subsection being questioned.

Annex G.
An example of encoding a frame for OFDM PHY. Table G.17-Last 144 bits scrambling.

3. The applicable conditions for the case in question.

In order to check if our design of the PHY is correct, we have check it by means of the example given in Annex G "An example of encoding a frame for OFDM PHY".

All our results match properly with those given in all the tables except for 'Table G.17-Last 144 bits after scrambling'. In this case, the bits number 818 and 820 which are in the standard are '0'. However, we obtain two '1'.

In order to check if the scrambler module works properly we have tried to obtain the 127-bit repetitive sequence given in page 16 in chapter '17.3.5.4. PLCP DATA scrambler and descrambler' and we do it correctly. As it can be saw, the values of the 7-bit shift register of the scrambler depends only on the seed. In the example given, the seed is '1011101' and we have checked as well that we match the 'Table G.15- Scrambling sequence for seed 1011101'. Therefore, in our opinion the mismatch in 'Table G.17' might be caused by the input of the scrambler, that is, the DATA bits. However, we are obtaining the same values than those given in 'Table G.14-Last 144 DATA bits'.

After all this explanation, i would be really grateful if you could confirm to us that the data showed at 'Table G.17' are completely correct or if there is any mistakes on it.

Interpretation for IEEE STD 802.11a-1999 (reaffirmed 2003)

In document 11-04-1198-00-00m, Inoue-san, et al, provide an analysis of the material in question in Annex G. This analysis is reproduced here.

• The two bits (bit#818 and bit#820) in the Table G.17 should be corrected
– Both of bit #818 and bit #820 in the Table G.17 are “0” in current standard.

– Both bit #818 and bit #820 should be modified to be “1”.
• Table G.1:
– Table G.1 consists of following items.
• The MAC header (24 octets)
• The first 72 characters of the original message converted to ASCII code
• The CRC32 (4 octets)
– A PSDU of length 100 octets (= 800 bits)
{04 02 00 2e 00 60 08 cd … 74 72 65 61 da 57 99 cd}

• Generation of DATA field in PPDU frame:
– The DATA field in a PPDU frame consists of SERVICE field, PSDU, tail (PPDU TAIL) and Pad bits.
– Table G.13 shows the first 144 bits of the DATA field.
• The SERVICE field (sixteen “0” bits) are added before PSDU.
– Table G.14 shows the last 144 bits of the DATA field.
• Assuming the modulation mode of 36M bps (16QAM, r=3/4), 42 Pad bits are appended in this case.

• Table G.15 – Scrambling sequence for seed 1011101
– This is the output sequence of the scrambler when the initial value of the shift register is 1011101.
– We have confirmed that the Table G.15 was correct.

• We have confirmed that:
– Table G.16 (First 144 bits after scrambling) was correct.
– Table G.17 (Last 144 bits after scrambling) was NOT correct as the requester pointed out.

• The bit #818 and bit #820 in the Table G.17 correspond to the PPDU TAIL bits.
• The PPDU TAIL bits and PAD bits are all “0”
o There will be exact sequence of the scrambler output after bit #816 in the Table G.17.
o The bits #818 and #820 in the Table G.17 correspond the bits #56 and #58 in the Table G.15 which have value of “1”.

The conclusion of this analysis is that two bits in table G.17 are in error. This error will be brought to the attention of the 802.11 working group to be addressed in the next revision of the standard.

Interpretation #13

Interpretation Number: 1-05/06 (short SYNC field value)
Topic: Accuracy of material 802.11g
Relevant Clauses: 19.3.2.5 (figure 153B), 18.2.3.8
Classification: Unambiguous

Interpretation Request

I think there is an error in "Figure 153B Short preamble PPDU format for DSSS-OFDM", page 23, of the document 802.11g-2003.pdf

In this figure, it is written : SYNC (56 bits - Scrambled Ones)

It's not coherent with the short preamble of 802.11b, which SYNC is (56 bits - Scrambled Zeros) and the text in the norm 802.11g is not coherent with the figure 153B. It should be SYNC (56 bits - Scrambled Zeros) in this figure.

The text is : 19.3.2.5 The short PLCP preamble and header are used to maximize the throughput by reducing the overhead associated with the preamble and header. Figure 153B shows the short preamble PLCP PPDU format. As seen, the PSDU is appended to the PLCP Preamble and the PLCP header. The short PLCP Preamble is described in 18.2.3.8 and 18.2.3.9.

In 18.2.3.8 (802.11b), the text is shortSYNC = 56 bits of scrambled "0" bits. So there is an error.

Interpretation Response

The standard is unambiguous on this issue. Figures are not normative and the description of the field occurs only once in the standard. Therefore the description of the short SYNC field is unambiguously defined to be scrambled zeros.

The working group will consider correcting the figure during the next revision of the standard.

Interpretation #14

Interpretation Number: 2-05/06 (use of 802.1X uncontrolled port by 802.11i)
Topic: conflicting statements in 802.11i on the use of the 802.1X uncontrolled port
Relevant Clauses: 5.4.2.2, 6.1.4, 8.5.4
Classification: Unambiguous

Interpretation Request

We have an interpretation request as follows:

1. The specific designation of the standard, including the year of publication: IEEE Std 802.11i 2004

2. The specific subsection being questioned

In Clause 5.4.2.2:
"However, a given protocol may need to bypass the authorization function and make use of the IEEE 802.1X Uncontrolled Port.”

In Clause 6.1.4:
"The IEEE 802.1X Controlled/Uncontrolled Ports discard the MSDU if the Controlled Port is not enabled or if the MSDU does not represent an IEEE 802.1X frame."

3. The applicable conditions for the case in question

Is a non-802.1X frame such an IP datagram allowed to make use of 802.1X Uncontrolled Port before Controlled Port is enabled in a certain case? The question comes up because IETF PANA WG is defining a mode in which PANA protocol messages, carried in IP datagrams, make use of 802.1X Uncontrolled Port over 802.11i.

It appears that there is a strict architectural boundary between 802.11i and 802.1X in that the 802.11i state machines order and filter events that are related to 802.1X so that 802.1X state machines can process them. If so, how 802.1X state machines process those events should be governed by 802.1X, not by 802.11i. In that sense, shouldn't the above quoted text in both Clause 5.4.2.2 and Clause 6.1.4 be interpreted as informative, not normative?

Interpretation Response

The standard is unambiguous on this issue. While 5.4.2.2 states a general capability of 802.1X, clause 6.1.4 places a limitation on this usage in 802.11. Clause 8.5.4 further specifies this limitation in an ESS:

In an ESS, the AP indicates that the IEEE 802.11 link is available by invoking the MLME-ASSOCIATE.indication or MLME-REASSOCIATE.indication primitive. At this point the Authenticator’s Controlled Port corresponding to the STA’s association is blocked, and communication of all non-IEEE 802.1X MSDUs sent or received via the Controlled Port is not authorized.

Interpretation #15

Interpretation Number: 1-07/06 (RTS/CTS with fragmentation)
Topic: ambiguity of RTS/CTS usage description with fragmentation
Relevant Clauses: 9.2.5.2, 9.2.5.3, 9.2.5.6, 9.2.5.7, 9.2.8, 9.7
Classification: Unambiguous

Interpretation Request

Clause 9.2.5.6 states that: RTS-CTS mechanism precedes the first fragment only in case of transmission of multiple fragments by a source STA, where (RTS threshold < Fragmentation Threshold). It also says "no further RTS/CTS frames need to be generated after the RTS/CTS that began the frame exchange sequence even though subsequent fragments may be larger than dot11RTSThreshols". The section also discusses the worst-case scenario, where an acknowledgment of a fragment is lost and is never heard by the source station.

How does the frame transmission begin when there is an acknowledgment loss? Will there be an RTS-CTS exchange by the source STA again before retrying the lost fragment?

Clause 9.2.5.6 says that the RTS-CTS mechanism should only occur before the transmission of the first fragment; the Frame Exchange Sequence in clause 9.7 also depicts this behavior, i.e. {RTS-CTS-}[Frag - ACK -]Last - ACK

However, clause 9.2.5.5 states: "When a source STA transmits a fragment, it shall release the channel, then immediately monitor the channel for an acknowledgment.

If no acknowledgment is received, then should the source STA perform a random backoff and contend for the channel? Would the source STA be required to send a RTS at this point to reserve the NAV again after gaining access on the channel?

The standard is not clear from these clauses what the desired behavior should be.

Interpretation Response

The standard is unambiguous on this issue. Clauses 9.2.5.2, 9.2.5.3, 9.2.5.7, and 9.2.8 describe the use of the backoff procedure in various situations, including that when an ACK is not received in response to an individually addressed data frame (fragment). The description of fragmentation in the standard does not modify this behavior. Therefore, the standard requires a backoff procedure to be performed after loss of an ACK frame.

Clause 9.2.6 describes the requirement to use RTS before the transmission of any MPDU longer than dot11RTSThrshold. Clause 9.2.5.6 modifies this general requirement when transmitting a fragment burst. RTS/CTS is required to precede the initial fragment in a fragment burst and is required not to be transmitted before any other fragments in that same fragment burst. Clause 9.7 also shows RTS/CTS preceding the initial fragment of a fragment burst.

The standard is unambiguous on the topic of RTS/CTS usage with fragmentation.

Interpretation #16

Interpretation Number: 1-09/06 (Unknown values in information elements)
Topic: requirements for operation of an implementation when encountering unknown values in an information element
Classification: Unambiguous

Interpretation Request

The current description of Information elements in 7.3.2 is vague about the processing of unknown element-specific information fields, in contrast with the processing of unknown information element fields:

A STA that encounters an unknown or reserved element ID value in a management frame received without error shall ignore that element and shall parse any remaining management frame body for additional information elements with recognizable element ID values.

An example would be an 802.11j conformant STA that receives a Country Information Element for Japan with a Regulatory Class value of 21, which was reserved at the time of 802.11j approval, but has subsequently become specified.

PROPOSAL

Change the current text to include the processing of unknown element-specific information fields:

A STA that encounters an unknown or reserved element ID value [or unknown element-specific information field] in a management frame received without error shall ignore that element [or unknown element-specific information field,] and shall parse any remaining management frame body for additional information elements with recognizable element ID values.

Interpretation Response

The standard is silent on this matter, in general. It does not specify any particular action to be taken by a compliant implementation in the situation described by the requester. There are specific requirements for some fields in some information elements, but not all.

This issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

Interpretation #17

Interpretation Number: 2-09/06 (use of short and long retry counters)
Topic: ambiguity of usage of short and long retry counters after RTS/CTS failure
Relevant Clauses: 9.2.5.3, 9.2.5.7, C.3
Classification: Ambiguous

Interpretation Request

Object:Request for interpretation for IEEE Std 802.11-1999 Clause:9.2.5.3.

According to clause 9.2.5.3 "After an RTS frame is transmitted, the STA shall perform the CTS procedure, as defined in 9.2.5.7. If the RTS transmission fails, the short retry count for the MSDU or MMPDU and the STA short retry count are incremented." However, in annex C.3 (page 348), in the case of a RTS failure, the only counters which are incremented are the long one's (the short one's are not modified in this case).

Are the annex and the clause in conflict?

Interpretation Response

The standard is ambiguous on this issue. Clause 9.2.5.3 and 9.2.5.7 describe the use of the use of the short and long retry counters, when the CTS is not received in response to a transmitted RTS. Annex C.3 also describes this operation. These two descriptions of the requirements of an implementation are in conflict with each other.

The standard is ambiguous on this issue. The issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

Interpretation #18

Interpretation Number: 1-09/07 (TCLAS Elements)

Topics: Usage of TCLAS Elements with (Classifier Elements, VLANs, TCP and UDP protocol)
Relevant Clauses: 7.3.2.29
Classification: Ambiguous

An interpretation is requested on the following aspects of TCLAS elements, as specified in section 7.3.2.29 of [1]:

Interpretation Request #1

Issues with Type 0 (Ethernet) TCLAS elements

1. Use of Type field for VLAN unclear
a. Can a Type value of 81-00 be used to match all VLAN-tagged frames, per Annex M, or does it only apply to the innermost Ethertype field in a frame?

Interpretation Response #1

IEEE Std. 802.11-2007 is unambiguous on this matter. The IEEE Std. 802.11-2007 does not apply special
meaning to the type value 81-00. From the normative material in Clause 7 of IEEE Std. 802.11-2007, the type value of 81-00 shall match all Ethernet packets with type value 81-00 without further interpretation of the meaning inherent in that value.

Interpretation Request #2

b. Can matching on Type be used with singly-encapsulated VLAN frames, i.e. those starting AA-AA-03-00-00-00-81-00 but not starting AA-AA-03-00-00-00-81-00-xx-yy-AA-AA, per Annex M (which is merely informative)?

Interpretation Response #2

IEEE Std. 802.11-2007 is unambiguous on this matter. Clause 7 defines the normative behaviour for TCLAS. Annex M contains informative information only and does not modify the normative behaviour defined in Clause 7.

Interpretation Request #3

2. Use with non-SNAP/non-RFC1042 frames unclear
a. Can matching on Type be used with non-RFC1042 SNAP frames, i.e. those starting AA-AA-03 but not starting AA-AA-03-00-00-00, per Annex M?
i. If so, does this mean that the first three octets of the SNAP header are simply ignored?
ii. If not, does this mean that AppleTalk (2), AppleTalk AARP (1) and IPX Ethernet II, per Table M.2, cannot be matched?
b. Can matching on Type be used with non-SNAP frames, e.g. those starting E0-E0-03 or FF-FF, per Annex M?
i. If so, how?

Interpretation Response #3

IEEE Std. 802.11-2007 specifies how to match the type field of an Ethernet packet without specifying any mapping from an Ethernet packet to a MAC-UNITDATA primitive. Whenever the integration function results in an Ethernet packet, a TCLAS classifier of Type 0 [Ethernet] may meaningfully be applied. Whenever an integration function does not result in an Ethernet packet, a TCLAS classifier of Type 0 cannot be applied.

Interpretation Request #4

Issues with Type 1 (TCP/UDP IP) TCLAS elements

1. Use of Version field unclear
a. Is the Version field part of the Classifier Mask, such that the LSB of the Classifier Mask refers to the Version, or does the LSB of the Classifier Mask refer to the Source IP Address?

b. Is the Version field required to be set to 4 for IPv4 or 6 for IPv6 (even if the answer to the previous question is that the LSB of the Classifier Mask refers to the Version and hence the Version may not be part of the matching), or is the IP version to which a Type 1 TCLAS element applies implied by the length of the TCLAS element?

Interpretation Response #4

1a) IEEE Std. 802.11-2007 is unambiguous on this matter. The version field is included in the list of classifier parameters [paragraph 4 page 137] and is therefore included in the classifier mask subfield as defined in [paragraph 1 page 137].

1b) IEEE Std. 802.11-2007 is unambiguous with respect to the fields included in the Frame Classifier. IEEE Std. 802.11-2007 is ambiguous with respect to the value contained in those fields. Specification of those values
is outside the scope of IEEE Std. 802.11-2007.

IEEE Std. 802.11-2007 is ambiguous on this issue. The issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

Interpretation Request #5

2. Lack of Protocol field for IPv6
a. It is not possible to match based on the upper-layer protocol in IPv6 frames, unlike in IPv4 frames. Is this an oversight, or is it deliberate?

Interpretation Response #5

2a) IEEE Std. 802.11-2007 is unambiguous on this issue. The next header field is not included in the IPv6 Frame Classifier.

This issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

3. Lack of DSCP field for IPv6
a. It is not possible to match based on the DSCP in IPv6 frames, unlike in IPv4 frames. Is this an oversight, or is this deliberate?

3a) IEEE Std. 802.11-2007 is unambiguous on this issue. The Traffic Class field is not included in the IPv6 Frame Classifier.

This issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

Interpretation Request #6

4. Setting of the 4 MSBs in Flow Label field for IPv6 unclear
a. It is not specified that the 4 MSBs in the Flow Label field for IPv6 are set to 0/ignored, unlike the 2 MSBs in the DSCP field for IPv4. Is this an oversight, or is this deliberate?

Interpretation Response #6

4a) IEEE Std. 802.11-2007 is ambiguous on this issue. The text does not describe how the 20-bit IPv6 Flow Label is aligned within the 24-bit Flow Label Field in figure 7-89.

This issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

Interpretation Request #7

5. Use of Source/Destination Port fields for protocols other than TCP and UDP unclear
a. The formatting of the specification suggests that in frames carrying protocols other than TCP or UDP, only the DSCP and Protocol (IPv4) or Flow Label (IPv6) fields are part of the matching. Is this unintended? [Will assume so!]

Interpretation Response #7

5a) IEEE Std. 802.11-2007 is unambiguous on this issue. The classifier mask allows the selection of version, source IP address, destination IP address, DSCP, and protocol. The text of IEEE Std. 802.11-2007 does not describe every possible combination of classifier mask settings.

Interpretation Request #8

b. Is it valid for a TCLAS element for IPv4 to have the Classifier Mask bit corresponding to the Protocol clear, but to have the bits corresponding to the Source and/or Destination Port set? [Will assume so, based on the inapplicability of this question to TCLAS elements for IPv6.]

Interpretation Response #8

5b) Yes this is valid. The text of IEEE Std. 802.11-2007 does not describe every possible combination of classifier mask settings.

Interpretation Request #9

c. If the Classifier Mask bits corresponding to the Source and/or Destination Port are set (and for IPv4 the Protocol bit is clear):

i. How are frames with protocols which do not have 16-bit source/destination ports handled? Do they never match, or do they match subject to the other fields selected in the Classifier Mask (and what if there are no other selected fields – do they then always match?)?

ii. How are frames with protocols other than TCP and UDP which do have 16-bit source/destination ports handled? Do they never match, or do they match subject to these and the other fields selected in the Classifier Mask, or do they match subject only to the other fields selected in the Classifier Mask? What if the classifying device does not know this protocol?

Interpretation Response #9

5c) (both i and ii) IEEE Std. 802.11-2007 is ambiguous on this issue. If the protocol is not TCP and not UDP then IEEE Std. 802.11-2007 does not state how source port and destination port classifier fields are used.

This issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

Whether this condition is diagnosed it is up to the SME and is out of scope for the IEEE Std. 802.11-2007. The IEEE Std. 802.11-2007 is ambiguous regarding how the SME communicates invalid TCLAS parameters to the requesting STA.

Interpretation Request #10

d. Is it valid for a TCLAS element for IPv4 to have the bits corresponding to the Protocol and to the Source and/or Destination Port set, where the Protocol is not TCP or UDP?
i.If it isn't, is the classifying device required to diagnose the condition, and if so what Status Code should it use?
ii. If it is:
1. What if the classifying device does not know this protocol? Is it required to diagnose the condition, and if so what Status Code should it use?
2. If the classifying device does know this protocol, what if it does not have d16-bit source/destination ports? Is the classifying device required to diagnose the condition, and if so what Status Code should it use?

Interpretation Response #10

5d) (both i and ii) IEEE Std. 802.11-2007 is ambiguous on this issue.If the protocol is not TCP and not UDP then IEEE Std. 802.11-2007 does not state how source port and destination port classifier fields are used.

This issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

Whether this condition is diagnosed it is up to the SME and is out of scope for the IEEE Std. 802.11-2007. The IEEE Std. 802.11-2007 is ambiguous regarding how the SME communicates invalid TCLAS parameters to the requesting STA.

Interpretation Request #11

Issues with Type 2 (IEEE 802.1D/Q) TCLAS elements

1. Number of fields unclear
a. The text implies that the 802.1D priority and the 802.1Q VLAN ID can be matched independently, but the figure implies that the classifier uses a single combined field (including the CFI bit). Which is the correct interpretation?

Interpretation Response #11

IEEE Std. 802.11-2007 is ambiguous on this issue. This issue will be forwarded to the 802.11 Working Group for consideration in a future revision of the standard.

Interpretation Number: #12 – 05/2008

Document: IEEE Std. 802.11-2007
Topic: Multiple SSID usage
Relevant Clauses: not specified
Relevant Figures: not specified
Classification: Ambiguous/Non-Ambiguous not specified by WG

Introduction:

Service Providers use Multi-SSID many ways:

- extra SSID for particular use-case, device-class, WEP...

- very important for non-enterprise (hotspots, homes…)

But…There are interop issues

-Beacon timing

- Some devices cannot cope with a variable or very-short beacon interval
  - no problems if 50mSec apart,
  - BUT t=SIF gives problems with some devices !
- Needs defining for multi-SSIDs
  - All clients need to cope with such timing

  - Spacing beacons by just SIFS/DIFS

Question:

If an AP device is generating multiple BSSID signals what is the proper spacing between those SSIDs?

Interpretation Request Response:

Std. IEEE 802.11-2007 only defines one MAC/PHY pair as a STA. When a product virtualizes multiple STAs within the same physical device, the interaction of the virtual STAs are currently outside the scope of the standard, however the use of multiple BSSID/SSID functionality is currently being defined.

The commenter (and others interested) is invited to come and participate with the 802.11 WG.

Interpretation Number: #13– 07/2008

Document: IEEE Std. 802.11-2007
Topic: Max SP Length subfield
Relevant Clauses: 7.1.1, 7.3.1.17
Relevant Figures: not specified
Classification: Ambiguous/non-Ambiguous not specified by WG

Introduction:

Section 7.3.1.17 of Std. IEEE 802.11-2007 says that the Max SP Length subfield of the QoS Info field is reserved when all four U-APSD flags are set to 0. Section 7.1.1 of Std. IEEE 802.11-2007 says that reserved fields and subfields are set to 0 upon transmission and are ignored upon reception.

Question:

If a non-AP STA sets all four U-APSD flags to 0 in the QoS Info field in the QoS Capability IE in the Association Request, and then uses an ADDTS Request to set up a deliveredenabled TS (and also sets up a trigger-enabled TS -- perhaps the same TS), how many buffered MSDUs and MMPDUs may the AP deliver to this non-AP STA during an SP triggered by this non-AP STA?

Interpretation Response:

Std. IEEE 802.11-2007 does not specify when the bits are set to 0, a maximum limit of how many MSDU or MMPDUs are buffered by an AP. Therefore the maximum number would be AP implementation dependent value and would be dependent on the amount of traffic buffered at the AP (See table 7-25 bit 5-6). A limit is prescribed only when Bit 5 and/or 6 are set to 1.

Interpretation Number: #14– 07/2008

Document: IEEE Std. 802.11-2007
Topic: Minimum PHY Rate definition
Relevant Clauses: 7.3.2.30
Relevant Figures: not specified
Classification: Ambiguous/non-Ambiguous was not specified by WG

An interpretation is requested on the following:

Section 7.3.2.20 {note: the TSPEC element subclause is 7.3.2.30} of IEEE Std. 802.11-2007says that the Minimum PHY Rate field of the TSPEC IE is “the desired minimum PHY rate to use for this TS, in bits per second, that is required for transport of the MSDUs belonging to the TS in this TSPEC.”

What are the exact semantics of this field?

Does this need to correspond to an operational rate of the AP which the non-AP STA can transmit at, for a TS with an uplink component (vice-versa for a TS with a downlink component)? [*]

If not, must it be a rate supported by the PHY being used (though perhaps not a rate supported by the non-AP STA and/or AP)?

If not, must it be less than or equal to the highest rate supported by the PHY being used? Or the highest rate supported by the non-AP STA and AP?

And if the answer to question marked with [*] is no, then how is K.2.2 to be used?

An example may help. Say we're using 802.11a, the AP supports 6, 12, 24 and 48 Mbps, and the STA supports 6, 9, 12 and 24 Mbps (here "supports" means both tx and rx). Which of the following values would be valid values in the Minimum PHY Rate field for an uplink TSPEC, and for those values, what value would be used for to compute the MPDUExchangeTime in section K.2.2 of [1]?

1. 24 000 000 (supported by both STAs)
2. 9 000 000 (not supported by AP)
3. 48 000 000 (not supported by non-AP STA)
4. 18 000 000 (valid .a rate, but not supported by either STA)
5. 36 000 000 (valid .a rate, but not supported by either STA and higher than non-AP STA's highest rate)
6. 27 000 000 (valid .a rate, but only in "half-clocked" operation)
7. 54 000 000 (highest rate on .a; not supported by either STA)
8. 1 111 111 111 (not a valid rate for any PHY; higher than highest rate on any PHY)
9. 111 111 111 (not a valid rate for any PHY; higher than highest rate on .a)
10. 11 111 111 (not a valid rate for any PHY, but in .a rate range)
11. 1 111 111 (not a valid rate for any PHY; lower than lowest rate on .a)
12. 111 111 (not a valid rate for any PHY; lower than lowest rate on any PHY)

13. 11 000 000 (not a valid .a rate, but valid .b rate and in .a rate range)
    1 000 000 (not a valid .a rate and not in .a rate range, but valid .b rate)

Interpretation Response:

In clause 7.3.2.30, the Minimum PHY Rate field definition:

- The Minimum PHY Rate field is 4 octets long and contains an unsigned integer that specifies the desired minimum PHY rate to use for this TS, in bits per second, that is required for transport of the MSDUs belonging to the TS in this TSPEC[21].

    - Footnote 21: This rate information is intended to ensure that the TSPEC parameter values resulting from an admission control negotiation are sufficient to provide the required throughput for the TS. In a typical implementation, a TS is admitted only if the defined traffic volume can be accommodated at the specified rate within an amount of WM occupancy time that the admissions control entity is willing to allocate to this TS.

The standard does not require the use any of the Operational Rates for the value of the Minimum PHY Rate.

K2.2 is part of an Informative Annex, and is provided to assist implementers, but it does not specify required functionality.