IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Text for Selective transmission of the Probe Response | | | | |
| Date: 2012-01-12 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jae Seung Lee | ETRI | 161 Gajeong-dong,  Yuseong-gu, Daejeon, Korea | +82 42 860 1326 | jasonlee@etri.re.kr |
| Minho Cheong | ETRI | 161 Gajeong-dong,  Yuseong-gu, Daejeon, Korea | +82 42 860 5635 | [minho@etri.re.kr](mailto:minho@etri.re.kr) |
| Je Hun Lee | ETRI | 161 Gajeong-dong,  Yuseong-gu, Daejeon, Korea | +82 42 860 3820 | [jhrhee@etri.re.kr](mailto:jhrhee@etri.re.kr) |
| Jabeom Gu | ETRI | 161 Gajeong-dong,  Yuseong-gu, Daejeon, Korea | +82 42 860 1776 | gjb@etri.re.kr |
| Jaewoo Park | ETRI | 161 Gajeong-dong,  Yuseong-gu, Daejeon, Korea | +82 42 860 5723 | parkjw@etri.re.kr |
| Seungkwon Cho | ETRI | 161 Gajeong-dong,  Yuseong-gu, Daejeon, Korea | +82 42 860 5794 | skcho@etri.re.kr |
| Hyun Gu Park | ETRI | 161 Gajeong-dong,  Yuseong-gu, Daejeon, Korea | +82 42 860 5886 | phg@etri.re.kr |
| Sok-kyu Lee | ETRI | 161 Gajeong-dong,  Yuseong-gu, Daejeon, Korea | +82 42 860 5919 | sk-lee@etri.re.kr |

Abstract

This document proposes normative text for FILS Scanning – Selective transmission of the Probe Response.

Changes in the text refer to: Draft P802.11-REVmb/D12.

This proposal provides normative text to make active scanning more efficiently by selective transmission of the Probe Response frame based on the capability and the preference of the requesting STAs.

* Filtering information based on capabilities and preferences of the STA is included in the Probe Request frame.
* If the STA that received the Probe Request can check the capabilities and preferences of the STA that transmitted the Probe Request.
* If the preference of the STA such as request for security processing, or request for no security processing or request for associate with HT, VHT, or non-HT STA cannot be satisfied by the responding STA, then Probe Response frame is not transmitted by the responding STA.
* Capability information such as security capability including RSN capability is included in the Probe Request frame. If the capability of the STAs that transmit Probe Request frame cannot fulfill the security policy of the responding STA that receives the Probe Request frame or the responding STA cannot accept the requesting STA because of the responding STA’s current condition (AP Load, etc..), then the responding STA does not respond with the Probe Response frame.
* Selective transmission of the probe response helps to reduce the traffic caused by Probe Response frames, and also helps to select appropriate STAs to be associated with in advance.
* Channel related information received in the probe responses during the active scanning process is used to select the next channel to be scanned.

**6.3.3 Scan**

**6.3.3.2.2 Semantics of the service primitive**

The primitive parameters are as follows:

MLME-SCAN.request(

BSSType,

BSSID,

SSID,

ScanType,

ProbeDelay,

ChannelList,

MinChannelTime,

MaxChannelTime,

RequestInformation,

SSID List,

ChannelUsage,

AccessNetworkType,

HESSID,

MeshID,

CapabilityFilterInfo,

VendorSpecificInfo

)

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| CapabilityFilterInfo | CapabilityFilterInfo element | As defined in 8.4.x. | Specifies options required for Probe Response frame filtering by the responder of the Probe Request based on the capabilities or preferences of the requesting STAs. This element is present only  if dot11FILSActivated is true. |

**8.3.3.9 Probe Request frame format**

**Table 8-26—Probe Request frame body**

|  |  |  |
| --- | --- | --- |
| **Order** | **Information** | **Notes** |
| xx | CapabilityFilterInfo | The CapabilityFilterInfo element is present only if dot11FILSActivated is true. |

**8.4.2.x CapabilityFilterInfo element**

The CapabilityFilterInfo element specifies options required for Probe Response frame filtering by the responder of the probe request based on the capabilities or preferences of the requesting STAs. This element is present only if dot11FILSActivated is true.

The format of the CapabilityFilterInfo element is shown in Figure 8-x.

|  |  |  |  |
| --- | --- | --- | --- |
| Element ID | Length | Filtering Preference | Security capability element |

Octets: 1 1 2 variable

**Figure 8-x— CapabilityFilterInfo element**

The Element ID field is equal to the CapabilityFilteringInfo value in Table 8-x.

The value of the Length field is the length of the Filtering Preference field and Security capability element in octets (variable).

Filtering Preference field specifies the filtering preferences of the STAs that transmit Probe Request frame.

The format of the Filtering Preference field is shown in Figure 8-x.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Filter Request | Require Security | Require No  Security | Require HT | Require  VHT | Require non-HT | Reserved |

bits: 1 1 1 1 1 1 10

**Figure 8-x—Filtering Preference field format**

Filter Request subfield indicates whether the STA prefers the filtering of the Probe Response frame by the responder of the Probe Request frame based on the CapabilityFilterInfo element that it transmits in the Probe Request frame.

If this field is set to 1, then the STA that is the responder of the probe request shall send the Probe Response frame if the responding STA can satisfy all the preferences of the requesting STA specified in the Filtering Preference field and if the Security capabilities included in the Security capability element sent by the requesting STA meets all the security policy of the responding STA and the supported rates of the requesting STA indicated in the Supported rates element in the Probe Request frame supports all the rates in the BSSBasicRateSet parameter of the responding STA.

If the Filter Request subfield is set to 0, then the Probe Response frame is transmitted by the responder of the probe request regardless of the preferences or capabilities of the requesting STA.

A requesting STA sets the Require Security subfield to 1 if it wants to use security options, and if this subfield is set to 1, then Security capability element shall be present in the CapabilityFilterInfo element that specifies the security capabilities of the requesting STA.

Require No Security subfield is set to 1 if the STA does not want to use any security options regardless of its security capabilities.

If the requesting STA has no security preference, then both the Require Security subfield and the Require No Security subfield shall be set to 1. In this case, the Security capability element shall be included in the CapabilityFilterInfo element to indicate the security capabilities of the requesting STA. If the responding STA does not require security options, then it responds with Probe Response frame, If the responding STA requires security options, it checks the Security capability element in the Probe Request frame and responds with Probe Response frame only if the security capabilities of the requesting STA meets the policy of the responding STA.

Table 8-x shows the meaning of the Require security subfield and Require No Security subfield.

**Table 8-x—Meaning of the Require Security and Require No Security subfield**

|  |  |  |
| --- | --- | --- |
| **Require Security** | **Require No Security** | **Meaning** |
| 1 | 1 | . No Security Preference by the requesting STA.  . Security capability element shall be included in the CapabilityFilterInfo element. |
| 1 | 0 | . The requesting STA requires the use of the security options.  . Security capability element shall be included in the CapabilityFilterInfo element. |
| 0 | 1 | . The requesting STA requires no security options to be used.  . Security capability element may not be included in the CapabilityFilterInfo element. |
| 0 | 0 | . Reserved. |

Table 8-x shows the meaning of the Require HT subfield, require VHT subfield, and Require non-HT subfield.

**Table 8-x—Meaning of the Require HT subfield, require VHT subfield, and Require non-HT subfield**

|  |  |  |  |
| --- | --- | --- | --- |
| **Require HT** | **Require VHT** | **Require non-HT** | **Meaning** |
| 1 | 1 | 1 | No preference. |
| 1 | 0 | 0 | The requesting STA requires to associate with only HT STAs. |
| 0 | 1 | 0 | The requesting STA requires to associate with only VHT STAs. |
| 0 | 0 | 1 | The requesting STA requires to associate with only non-HT STAs. |
| 1 | 1 | 0 | The requesting STA requires to associate with HT STAs or VHT STAs. |
| 1 | 0 | 1 | The requesting STA requires to associate with HT STAs or non-HT STAs. |
| 0 | 1 | 1 | The requesting STA requires to associate with VHT STAs or non-HT STAs. |
| 0 | 0 | 0 | Reserved. |

Security capability element specifies the security capabilities of the STAs that transmit Probe Request frame.

The format of the Security capability element is shown in Figure 8-x.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Element ID | Length | Version | Group Data Cipher Suite Count | Group Data Cipher Suite List | Pairwise Cipher Suite Count | Pairwise Cipher Suite List | AKM Suite Count | AKM Suite List |

Octets: 1 1 2 2 4 x m 2 4 x n 2 4 x o

|  |  |  |
| --- | --- | --- |
| RSN Capabilities | Group Management Cipher Suite Count | Group Management Cipher Suite List |

Octets: 2 2 4 x p

**Figure 8-x—Security capability element**

In Figure 8-x, mdenotes the group data cipher suite count, ndenotes the pairwise cipher suite count, o denotesthe AKM suite count, and p denotes the group management cipher suite count.

The Element ID field is equal to the Security capability value in Table 8-x.

The value of the Length field is the length of the Security capability element in octets.

Version, Pairwise Cipher Suite Count, Pairwise Cipher Suit List, AKM Suite Count, AKM Suite List, RSN Capabilities fields are the same fields used in the RSN element (See 8.4.2.27).

The Group Data Cipher Suite Count field indicates the number of Group data cipher suite selectors that are contained in the Group Data Cipher Suite List field. Group data cipher suite is used by BSS to protect group addressed frames.

The Group Management Cipher Suite Count field indicates the number of Group management cipher suite selectors that are contained in the Group Management Cipher Suite List field. Group management cipher suite is used by BSS to protect group addressed robust management frames.

If the requesting STA supports a Cipher Suite but if it does not want to use it with the STAs that it wants to transmit Probe Request frame, then it may not include it in the Security capability element.

**Table 8-54—Element IDs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Element** | **Element ID** | **Length of indicated element (in octets)** | Extensible |
| CapabilityFilterInfo element | xx | 2 to 257 |  |
| Security capability element | xx | 2 to 257 |  |

**10.1.4.3 Active scanning**

**10.1.4.3.x Sending a probe request**

If the requesting STA wants to apply Probe Response filtering by the responding STAs, it includes CapabilityFilterInfo element that specifies capabilities and preferences of the STA in the probe request when the dot11FILSActivated is true.

**10.1.4.3.x Sending a probe response**

An associated mesh STA that receives a Probe Request frame shall not respond with a Probe Response frame when dot11RadioMeasurementActivated is true and the Probe Request frame contains a DSSS Parameter Set element with its Current Channel field value different from the value of dot11CurrentChannelNumber.

Probe Response frames shall be sent as directed frames to the address of the STA that generated the probe request. The SSID List element shall not be included in a Probe Request frame in an IBSS.

STA supports it. In an improperly formed Request element, a STA may ignore the first element requested that is not ordered properly and all subsequent elements requested. In the probe response frame, the STA shall return the requested elements in the same order as requested in the Request element.

If dot11RadioMeasurementActivated is true and if the Request element of the Probe Request includes the RCPI element ID, the STA shall include in the Probe Response an RCPI element containing the measured RCPI value of the received Probe Request frame. If no measurement result is available, the RCPI value shall be set to indicate that a measurement is not available.

Additionally, if the dot11FILSActivated is true and if the CapabilityFilterInfo element is included in the Probe Request frame, the responding STA shall respond with a probe response only if following conditions are met:

1. Filter Request subfield in the CapabilityFilterInfo element is set to 0 or if b) and c) are satisfied.
2. Filter Request subfield in the CapabilityFilterInfo element is set to 1 and
3. The responding STA satisfies the security processing preferences specified in Require Security subfield and Require No security subfield in the CapabilityFilterInfo element (See Table 8-x for the meaning of the subfields), and
4. The responding STA satisfies the preferences specified in Require HT subfield, Require VHT subfield, and Require non-HT subfield in the CapabilityFilterInfo element (See Table 8-x for the meaning of the subfields), and
5. The security capabilities of the requesting STA satisfies the security policy of the responding STA when the Require Security subfield is set to 1 and Require No Security subfield is set to 0. If both the Require Security subfield and Require No Security subfield are both set to 1, and if the responding STA chooses to use security processing with the requesting STA, then the responding STA responds with Probe Response frame only if the security capabilities of the requesting STA satisfies the security policy of the responding STA and 1) and 2) are met. If both the Require Security subfield and Require No Security subfield are both set to 1, and if the responding STA does not choose to use security processing with the requesting STA, then the responding STA responds with Probe Response frame if 1) and 2) are met. In this case, it is not necessary to check the security capabilities of the requesting STA.

The security capabilities of the requesting STA does not satisfy the security policy of the responding STA if

1. The responding STA is an AP and Group Data Cipher Suite or Pairwise Cipher Suite or AKM Suite or Group Management Cipher Suite that are required by the AP is not included in the Security capability element or
2. The responding STA is an AP, and the AP supports CCMP or the AP is an HT STA, and the requesting STA is an HT STA but it supports only old cipher suite such as TKIP or WEP-40 or WEP-104, or
3. The responding STA is an AP and the AP is RSNA-enabled and wants to use RSNA with the requesting STA, but the values of MFPC and MFPR in the RSN capabilities included in the Security capability element sent by the requesting STA are not suitable for the AP to associate with the requesting STA, or
4. The responding STA is an IBSS STA and the requesting STA and the responding STA do not support a common subset of pairwise cipher suites or a common single group cipher suite or common AKM Suite, or
5. The responding STA is an IBSS STA, and the responding IBSS STA supports CCMP or the responding IBSS STA is an HT STA, and the requesting STA is an HT STA but it supports only old cipher suite such as TKIP or WEP-40 or WEP-104, or
6. The responding STA is an IBSS STA and the STA is RSNA-enabled and wants to use RSNA with the requesting STA, but the values of MFPC and MFPR in the RSN capabilities included in the Security capability element sent by the requesting STA are not suitable for the responding IBSS STA to associate with the requesting STA, or
7. The responding STA is a Mesh STA and the requesting STA and the responding Mesh STA do not support a common subset of pairwise cipher suites or a common single group cipher suite, or
8. The responding STA is a Mesh STA and the requesting STA supports only old cipher suite such as TKIP or WEP-40 or WEP-104 as a pairwise cipher suite or a group cipher suite.
9. Filter Request subfield in the CapabilityFilterInfo element is set to 1 and the supported rates of the requesting STA indicated in the Supported rates element in the Probe Request frame supports all the rates in the BSSBasicRateSet parameter of the responding STA.

If the responding STA decides that it cannot accept the requesting STAs because of some reasons, such as high load of the responding STA, then it does not respond with Probe Response frame to prevent the association of the requesting STAs. How to decide whether the STA can accept the association request or not is out of scope of this standard.

**10.1.4.3.3 Active scanning procedure**

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure:

For each channel to be scanned:

a) Wait until the ProbeDelay time has expired or a PHYRxStart.indication primitive has been received.

b) Perform the Basic Access procedure as defined in 9.3.4.2.

c) Send a probe request to the broadcast destination address, with the SSID and BSSID from the MLME-SCAN.request primitive. When the SSID List is present in the MLME-SCAN.request primitive, send one or more probe request frames, each with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive.

d) Set to 0 and start a ProbeTimer.

e) If PHY-CCA.indication (busy) primitive has not been detected before the ProbeTimer reaches MinChannelTime, then set NAV to 0 and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses.

f) Set NAV to 0 and scan the next channel. If AP Channel Report element is included in the received probe responses, then a channel in the ChannelList that is also included in the AP Channel Report element that is not scanned yet may be selected as the next channel to be scanned. The AP Channel Report element included in the most recently received probe response is used.

When all channels in the ChannelList have been scanned, the MLME shall issue an MLME-SCAN.confirm

primitive with the BSSDescriptionSet containing all of the information gathered during the scan.