IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Draft Text for 11.55 eBCS Info | | | | |
| Date: 2020-06-23 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Hitoshi Morioka | SRC Software | Fukuoka, JAPAN |  | [hmorioka@src-soft.com](mailto:hmorioka@src-soft.com) |
| Antonio de la Oliva | InterDigital | Madrid, Spain |  | aoliva@it.uc3m.es |

Abstract

This document describes a draft text proposal for eBCS Info frame transmission and reception.

11. MLME

11.55 Enhanced Broadcast Service (eBCS) procedures

11.55.1 General

This subclause describes enhanced Broadcast Services (eBCS) procedures that are used for eBCS STAs.

eBCS is only supported in a non-DMG non-S1G infrastructure BSS.

eBCS can be used for both directions, downlink (eBCS DL) and uplink (eBCS UL). eBCS DL means broadcast from an eBCS AP to eBCS non-AP STAs. eBCS UL means broadcast from an eBCS non-AP STA to eBCS APs.

11.55.2 eBCS DL procedures

11.55.2.1 General

The eBCS DL uses three types of frame authentication mechanism as following.

* PKFA (12.15.2 Public Key Frame Authentication)
* HCFA (12.15.3 Hash Chain Frame Authentication)
* HLSA (12.15.4 No frame authentication with mandatory higher layer source authentication)

eBCS DL uses both eBCS Info frame and eBCS Data frame.

In addition to these frames, Management frames are optionally used.

The frame sequence is shown in Figure 11-bc1 (eBCS DL frame sequence).

スクリーンショット が含まれている画像

自動的に生成された説明

**Figure 11-bc1 eBCS DL frame sequence**

11.55.2.2 eBCS DL capability indications

The eBCS AP shall include the eBCS Capability element (9.4.2.\* eBCS Capability element) in Beacon and Probe Response frames. The eBCS Capability element indicates the next eBCS Info transmission time in units of Beacon Interval. For example, when the next eBCS Info transmission time is 5, the eBCS Info frame will be transmitted between next 5th Beacon and 6th Beacon.

When the eBCS non-AP STA that is scanning eBCS APs receives the Beacon frame or the Probe Response frame that include the eBCS Capability element, the eBCS non-AP STA should wait for the next eBCS Info. The eBCS non-AP STA may go into power save mode or move to other channel while waiting the next eBCS Info frame.

11.55.2.3 eBCS Info frame generation and usage

The eBCS Info frame is transmitted periodically in the interval of dot11BeaconPeriod \* dot11EBCSInfoInterval.

The eBCS Info frame contains the following information.

* eBCS Info Sequence Number
* Timestamp
* Fragment Control
* Fragment Hash Values (if fragmented)
* eBCS Info Interval
* Certificate of the AP (optional if HLSA is used for all contents, otherwise mandatory)
* Content Information
* Signature (optional if HLSA is used for all contents, otherwise mandatory)

The eBCS Info Sequence Number is initialized by a 64bit unsigned integer at the time of starting eBCS AP and incremented by every eBCS Info frame generation. If the eBCS Info Sequence Number overflows, it is set to 0.

The Timestamp is the time in UTC of generating the eBCS Info frame.

The Fragment Control indicates the total number of the fragmented frames and the index of the eBCS Info frame. The fragmentation procedure is described in 11.55.2.4 (eBCS Info fragmentation).

The Fragment Hash Values are present if the eBCS Info frame is fragmented and the fragment sequence number is 0.

The eBCS Info Interval is the interval of the eBCS Info transmission configured in dot11EBCSInfoInterval.

The Certificate of the AP is the X.509 certificate of the eBCS AP.

Details of the Signature is described in 12.15 (Frame authentication for eBCS).

An eBCS Info frame may contain multiple Content Information.

Each Content Information contains the following items.

* Authentication Algorithm
* Allowable Time Difference
* Broadcast Service ID
* Title
* Negotiation method
* Higher Layer Destination Address
* Time to Termination
* Next Schedule
* HCFA Base Key (in case of HCFA)
* Previous Period HCFA Base Keys (in case of HCFA, optional)
* HCFA Key Change Interval (in case of HCFA)
* Instant Authenticators (in case of HCFA, optional)
* Data (in case of PKFA, optional)

The Authentication Algorithm is either PKFA or HCFA with the public key algorithm and hash algorithm if required.

The Allowable Time Difference is the allowable time difference between the eBCS AP and the eBCS non-AP STAs. It depends on the frame authentication algorithm.

The Broadcast Service ID is the identifier of the content.

The Title is the human readable title of the content.

The Negotiation method is used to indicate the negotiation method that should be used to negotiate for the continuation of the broadcast service beyond the time of termination.

The Higher Layer Destination Address is the higher layer destination address of the content.

The Time to Termination is used to indicate the remaining time left at which the content will terminate unless additional negotiation is conducted by the initiator of the broadcast service or by other users of the content.

The Next Schedule is used to indicate the next time the content is scheduled to be transmitted.

The HCFA Base Key, the Previous Period HCFA Base Keys and the Instant Authenticators are used only in HCFA. The details are described in 12.15.3 (eBCS hash chain frame authentication (HCFA)).

The Data is the piggy-backed data. It is used only in PKFA.

On reception of the eBCS Info frame, the eBCS non-AP STA shall check the integrity of the eBCS Info frame as described in 12.15 (Frame authentication for eBCS) if the Certificate of the AP is included in the eBCS Info frame.

If the integrity of the eBCS Info frame is verified, the eBCS non-AP STA processes each Content Information according to the Authentication Algorithm.

* Common in all autientication algorithms,
  + Cache the Title, the Negotiation Method, the Higher Layer Destination Address, the Time to Termination and the Next Schedule.
  + Notify the cached information to SME through SME-MLME SAP as described in 6.3.\* (eBCS Content Information).
* In case of PKFA,
  + If the Data is present in the Content Information, forward the MSDU in the Data to higher layer. Otherwise, the Certificate in the eBCS Info frame shall be cached.
* In case of HCFA,
  + The HCFA Base Key in the Content Information shall be cached.
  + If the Instant Authenticators are present in the Content Information, the Instant Authenticators shall be cached.
  + If the Previous Period HCFA Base Keys are present in the Content Information, authenticate the eBCS Data frames of the previous HCFA period.

11.55.2.3 eBCS Info frame fragmentation (or in 10.4)

An eBCS Info frame may be fragmented into multiple MPDUs. The length of each fragment shall be equal number of octets for all fragments except the last, which may be smaller. The length of each fragment shall be an even number of octets, except for the last fragment. The length of a fragment shall never be larger than dot11FragmentationTreshold.

The fragmentation procedure is following.

1. Construct an eBCS Info frame and determine the length of fragments.
2. When the eBCS Info frame is fragmented to N MPDUs, the fragmentation number is set to N-1.
3. Insert a space for N-1 Fragment Hash Values to the eBCS Info frame.
4. Each fragment contains the eBCS Sequence Number, the Timestamp and the Fragment Control.
5. Divide the eBCS Info frame after the Fragment Hash Values into fragments.  
   The Fragment Hash Values, the Certificate and the Signature shall be contained in the first fragment.
6. The fragmentation number in the Fragment Control is set to the number of the fragments.
7. The fragmentation index in the Fragment Control is set to 0 (the first) to N-1 (the last) respectively.
8. Calculate the hash value of each fragment except the first one and put into the Fragment Hash Values.
9. Calculate and fill the signature of the first fragment.
10. Transmit the fragments consecutively.

The eBCS Info frame fragmentation is shown in Figure 11-bc2 (eBCS Info frame fragmentation).

スクリーンショットの画面

自動的に生成された説明

**Figure 11-bc2 eBCS Info frame fragmentation**

11.55.2.4 eBCS Info frame defragmentation (or in 10.4)

When the eBCS non-AP STA receives the eBCS Info frame with the Fragmentation Number in the Fragment Control is not 0 and the Fragmentation Index is 0, the eBCS non-AP STA shall verify the signature. If the verification succeeds, the eBCS non-AP STA shall cache the eBCS Info Sequence Number, Timestamp, the Fragment Control and the Fragment Hash Values.

When the eBCS non-AP STA receives the subsequent fragments of the eBCS Info frame, the eBCS non-AP STA shall check the integrity of the fragments by the following procedure.

1. The eBCS Info Sequence Number, the Timestamp and the Fragmentation Number in the Fragment Control in the received fragment are equal to that in the first fragment. If the values are different, the received fragment shall be discarded.
2. Calculate the hash value of the received fragment and compare it with the hash value in the Fragment Hash Values in the first fragment. If the hash value is different, the received fragment shall be discarded.
3. Cache the Content Information of the received fragment.

After all fragments are received, the eBCS non-AP STA concatenates the fragments and process the eBCS Info frame.

Straw poll

Which do you prefer about the location of the description for eBCS Info fragmentation/defragmentation?

1. Clause 11.55 (as this document)
2. Clause 10.4 (MSDU and MMPDU fragmentation) and 10.5 (MSDU and MMPDU defragmentation)