IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution to CIDs related to FST/architecture |
| Date: 2012-01-30 |
| Author(s): |
| Name | Company | Address | Phone | Email |
| Carlos Cordeiro | Intel |  |  |  |
| Brian Hart | Cisco |  |  |  |
| Adrian Stephens | Intel |  |  |  |
| Mark Hamilton | Polycom |  |  |  |
| Solomon Trainin | Intel |  |  |  |

Abstract

This document proposes resolutions to the following CIDs: 6505, 6276, 6503, 6277, 6384, 6175, 6082, 6323, 6151, 6504, 6257. The proposed resolution to each of them is REVISED, with the resolution text included below.

### 4.9.4 Reference model for multi-band operation

***Change the first para and Figure 4-16b as follows, and insert Figure 4-16c***

CID6277

The reference model of a device that is multi-band capable (see 10.32 Multi-band Operation) and that supports transparent FST is shown in Figure 4-16b. The reference model of a device that is multi-band capable and that supports non-transparent FST is shown in Figure 4-16c.



Figure 4-16b –Reference model for a multi-band capable device (transparent FST)



Figure 4-16c – Reference model for a multi-band capable device (non-transparent FST)

***Insert after the fifth paragraph***

CID6505 CID6323 CID6151

When used in the context of FST, the term session refers to non-PHY state information kept in a pair of STAs that communicate directly (i.e., excludes forwarding) and that is available prior to and following a session transfer. This state information is different depending if transparent or non-transparent is used. For transparent FST there is a shared multi-band management entity that has access to the local information within each SME, and in this case the state information includes BA agreements, TSs, association state, RSNA, security keys, sequence counter and PN counter. For non-transparent FST, the function of the multi-band management entity is restricted to coordinating the set up and tear down of a session transfer with no access to other local information within each SME. Therefore, with non-transparent FST any information local to an SME needs to be reestablished for the new band/channel and this can be done either prior to or following the session transfer (see 10.32).

***Change the eighth and ninth paras as follows***

As described in 5.1.5, a MAC address is not unique within the multi-band capable device when transparent FST is intended to be used. When transparent FST is used, a single MAC SAP at each peer is presented to the higher layers of that peer for all the frequency bands/channels that are identified by the same MAC address at that peer. When non-transparent FST is used, different MAC SAPs are presented to higher layers since different MAC addresses are used prior to and following an FST session transfer. Therefore when non-transparent FST is used, higher layers are responsible for managing the session transition between different frequency bands/channels. CID6504

Each MAC SAP is controlled by a separate and independent RSNA key management entity and 802.1X Authenticator/Supplicant, unless if transparent FST is used in which case the multi-band management entity is responsible for coordinating with each of the SMEs to ensure that a single RSNA key management entity and 802.1X Authenticator/Supplicant is shared among the MAC SAPs, and that a single 802.1X entity is controlled.

### 5.1.5 MAC data service architecture

CID6257 CID6276 CID6503 CID6175

***Change the first and second paragraphs as follows***

The MAC data plane architecture (i.e., processes that involve transport of all or part of an MSDU) is shown in Figure 5-1a for when transparent FST (10.32) is used and shown in Figure 5-1 otherwise. During transmission, an MSDU goes through some or all of the following processes: MSDU rate limiting, aggregate MSDU (A-MSDU) aggregation, frame delivery deferral during power save mode, sequence number assignment, fragmentation, encryption, integrity protection, frame formatting, and aggregate MAC protocol data unit (A-MPDU) aggregation. When transparent FST is used, an MSDU goes through an additional transparent FST entity that contains a demultiplexing process that forwards the MSDU down to the selected TX MSDU Rate Limiting process and thence futher MAC data plane processing. IEEE Std 802.1X-2004 may block the MSDU at the Controlled Port. At some point, the data frames that contain all or part of the MSDU are queued per AC/TS.

During reception, a received data frame goes through processes of possible A-MPDU deaggregation, MPDU header and cyclic redundancy code (CRC) validation, duplicate removal, possible reordering if the Block Ack mechanism is used, decryption, defragmentation, integrity checking, and replay detection. After replay detection (or defragmentation if security is not used), possible A-MSDU deaggregation, and possible MSDU rate limiting, one or more MSDUs are, delivered to the MAC\_SAP or to the DS. When transparent FST is used, MSDUs originating from different PHY-SAPs go through an additional transparent FST entity that contains a multiplexing process before forwarding the MSDU to the MSDU rate limiting process. The IEEE 802.1X Controlled/Uncontrolled Ports discard any received MSDU if the Controlled Port is not enabled and if the MSDU does not represent an IEEE 802.1X frame. Frame order enforcement provided by the enhanced data cryptographic encapsulation mechanisms occurs after decryption, but prior to MSDU defragmentation; therefore, defragmentation fails if MPDUs arrive out of order.

When transparent FST is used, the same security keys, sequence counter and PN counter are used by the MAC data plane to encrypt the MPDU prior to and following an FST session transfer, and the same security keys are used to check the integrity and perform the protection of MSDUs. When non-transparent FST is used, independent RSNAs, security keys, sequence counters and PN counters have to be established for each MAC data plane to be used prior to and following an FST session transfer. When transparent FST is used, a single MAC SAP at each peer is presented to the higher layers of that peer for all the frequency bands/channels that are identified by the same MAC address at that peer. When non-transparent FST is used, different MAC SAPs are presented to higher layers since different MAC addresses are used prior to and following an FST session transfer.

***Insert the following after Figure 5-1***



**Figure 5-1a – MAC data plane architecture (transparent FST)**

### 11.5.16.1 General

CID6082 CID6384

***Change the last paragraph as follows***

If the pairwise and group cipher suites used by a pair of multi-band capable devices to communicate with each other in the current operating band/channel is also supported after the transfer to another band/channel that was performed using transparent FST, the devices shall continue using the same cipher suites to communicate with each other after the transfer. In all other cases, a separate RSNA has to be established for the other band/channel (see 11.5.19).

***Remove the following para in 8.4.2.27.2 (P154L12) “***The cipher suite selectors 00-0F-AC:0, 00-0F-AC:1, 00-0F-AC:2, 00-0F-AC:4, and 00-0F-AC:5 are not valid cipher suite values for a DBand STA (11.3.1 Overview).***”***