



Multi-AP Specification Version 2.0

WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE

This document may be used with the permission of Wi-Fi Alliance under the terms set forth herein. By your use of the document, you are agreeing to these terms. Unless this document is clearly designated as an approved specification, this document is a work in process and is not an approved Wi-Fi Alliance specification. This document is subject to revision or removal at any time without notice. Information contained in this document may be used at your sole risk. Wi-Fi Alliance assumes no responsibility for errors or omissions in this document. This copyright permission does not constitute an endorsement of the products or services. Wi-Fi Alliance trademarks and certification marks may not be used unless specifically allowed by Wi-Fi Alliance.

Wi-Fi Alliance has not conducted an independent intellectual property rights ("IPR") review of this document and the information contained herein, and makes no representations or warranties regarding IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions.

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described herein, provided any duplication in whole or in part includes the copyright notice and the disclaimer text set forth herein. Unless prior written permission has been received from Wi-Fi Alliance, any other use of this document and all other duplication and distribution of this document are prohibited. Unauthorized use, duplication, or distribution is an infringement of Wi-Fi Alliance's copyright.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY WI-FI ALLIANCE AND WI-FI ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENT AND ANY INFORMATION CONTAINED IN THIS DOCUMENT.

Document revision history

Version	Date YYYY-MM-DD	Remarks
1.0	2018-06-18	Initial release.
2.0	2019-12-18	Updated with Profile-2 features

Table of contents

1	OVERVIEW.....	9
1.1	Scope	9
1.2	Purpose	9
2	REFERENCES	10
3	DEFINITIONS AND ACRONYMS	11
3.1.1	Shall/should/may/might word usage	11
3.1.2	Conventions	11
3.1.3	Definitions	11
3.1.4	Abbreviations and acronyms.....	13
4	ARCHITECTURE.....	15
4.1	Multi-AP architecture.....	15
4.1.1	Multi-AP example deployment	15
5	MULTI-AP ONBOARDING	19
5.1	1905 Push Button Configuration method	19
5.2	PBC Backhaul STA onboarding procedure.....	19
6	MULTI-AP DISCOVERY	22
6.1	Multi-AP controller discovery	22
6.2	Multi-AP service discovery.....	23
6.3	Client association and disassociation notification.....	23
7	MULTI-AP CONFIGURATION.....	25
7.1	AP configuration.....	25
7.2	AP operational BSS reporting	27
7.3	Policy configuration	27
8	CHANNEL SELECTION	29
8.1	Channel Preference Query and Report	29
8.2	Channel Selection Request and Report.....	29
8.2.1	Coordinated DFS CAC.....	31
8.2.2	DFS CAC Scan Requirements on a Multi-AP Controller	31
8.2.3	DFS CAC Scan Requirements on a Multi-AP Agent	31
9	CAPABILITY INFORMATION REPORTING	33
9.1	AP capability	33
9.2	Client capability	33
9.3	Backhaul STA capability	34
10	LINK METRIC COLLECTION.....	35
10.1	Backhaul link metrics	35
10.2	Per-AP metrics and bulk STA metrics.....	35
10.2.1	Link metric measurements from the AP	35
10.2.2	Channel Scan.....	36
10.3	Per-STA measurements.....	38
10.3.1	Associated STA link measurements from the AP	38
10.3.2	Unassociated STA RCPI measurements from the AP.....	39
10.3.3	802.11 beacon measurements from the client.....	40
10.4	Combined infrastructure metrics	40
11	CLIENT STEERING.....	42
11.1	Multi-AP Controller initiated steering mandate	42
11.2	Multi-AP Controller initiated steering opportunity.....	42
11.3	Multi-AP Agent initiated RCPI-based steering	43
11.3.1	RCPI-based steering rules.....	43
11.4	Multi-AP Agent determination of target BSS.....	43

11.5	Steering mechanisms.....	43
11.6	Client association control mechanism.....	44
11.7	Wi-Fi Agile Multiband and Tunneled Message support	45
12	BACKHAUL OPTIMIZATION.....	47
12.1	Backhaul optimization by backhaul station association control	47
13	MULTI-AP MESSAGING SECURITY	49
14	FOUR-ADDRESS MAC HEADER FORMAT.....	50
14.1	Wi-Fi backhaul frame and address handling.....	50
14.1.1	Receiver requirements	50
14.1.2	Transmitter requirements	50
14.1.3	Wired backhaul frame and address handling	51
15	MULTI-AP CONTROL MESSAGING RELIABILITY	52
15.1	CMDU reliable multicast transmission	52
15.1.1	CMDU reliable multicast transmission procedures	52
15.1.2	CMDU reliable multicast reception procedures	52
16	HIGHER LAYER DATA PAYLOAD OVER 1905	53
17	MULTI-AP CONTROL MESSAGING	54
17.1	Multi-AP message format.....	54
17.1.1	1905 AP-Autoconfiguration Search message format (extended)	61
17.1.2	1905 AP-Autoconfiguration Response message format (extended)	61
17.1.3	1905 AP-Autoconfiguration WSC message format (extended)	61
17.1.4	1905 Topology Response message format (extended).....	61
17.1.5	1905 Topology Notification message format (extended)	62
17.1.6	AP Capability Query message format.....	62
17.1.7	AP Capability Report message format.....	62
17.1.8	Multi-AP Policy Config Request message format	62
17.1.9	Channel Preference Query message format	62
17.1.10	Channel Preference Report message format	62
17.1.11	Channel Selection Request message format	62
17.1.12	Channel Selection Response message format.....	63
17.1.13	Operating Channel Report message format	63
17.1.14	Client Capability Query message format	63
17.1.15	Client Capability Report message format	63
17.1.16	AP Metrics Query Message format.....	63
17.1.17	AP Metrics Response Message format.....	63
17.1.18	Associated STA Link Metrics Query message format	63
17.1.19	Associated STA Link Metrics Response message format	63
17.1.20	Unassociated STA Link Metrics Query message format	64
17.1.21	Unassociated STA Link Metrics Response message format.....	64
17.1.22	Beacon Metrics Query message format	64
17.1.23	Beacon Metrics Response message format	64
17.1.24	Combined Infrastructure Metrics message format.....	64
17.1.25	Client Steering Request message format	64
17.1.26	Client Steering BTM Report message format	64
17.1.27	Client Association Control Request message format	65
17.1.28	Steering Completed message format	65
17.1.29	Backhaul Steering Request message format	65
17.1.30	Backhaul Steering Response message format.....	65
17.1.31	Higher Layer Data message format.....	65
17.1.32	1905 Ack message format	65
17.1.33	Channel Scan Request message format	65
17.1.34	Channel Scan Report message format.....	65
17.1.35	CAC Request message format	65
17.1.36	CAC Termination message format.....	65
17.1.37	Error Response message format.....	66

17.1.38	Topology Query message format.....	66
17.1.39	Association Status Notification message format.....	66
17.1.40	Tunneled message format	66
17.1.41	Client Disassociation Stats message format	66
17.1.42	Backhaul STA Capability Query message format.....	66
17.1.43	Backhaul STA Capability Report message format.....	66
17.1.44	Failed Connection message	66
17.2	Multi-AP TLVs format	67
17.2.1	SupportedService TLV format.....	67
17.2.2	SearchedService TLV format.....	67
17.2.3	AP Radio Identifier TLV format	67
17.2.4	AP Operational BSS TLV format.....	67
17.2.5	Associated Clients TLV format.....	68
17.2.6	AP Capability TLV format.....	68
17.2.7	AP Radio Basic Capabilities TLV format	69
17.2.8	AP HT Capabilities TLV format	69
17.2.9	AP VHT Capabilities TLV format.....	70
17.2.10	AP HE Capabilities TLV format.....	71
17.2.11	Steering Policy TLV format	72
17.2.12	Metric Reporting Policy TLV format	73
17.2.13	Channel Preference TLV format	74
17.2.14	Radio Operation Restriction TLV format.....	75
17.2.15	Transmit Power Limit TLV format	76
17.2.16	Channel Selection Response TLV format.....	76
17.2.17	Operating Channel Report TLV format	77
17.2.18	Client Info TLV format	77
17.2.19	Client Capability Report TLV format	77
17.2.20	Client Association Event TLV format	78
17.2.21	AP Metric Query TLV format.....	78
17.2.22	AP Metrics TLV format.....	78
17.2.23	STA MAC Address Type TLV format.....	79
17.2.24	Associated STA Link Metrics TLV format	79
17.2.25	Unassociated STA Link Metrics Query TLV format	80
17.2.26	Unassociated STA Link Metrics Response TLV format.....	80
17.2.27	Beacon Metrics Query TLV format.....	81
17.2.28	Beacon Metrics Response TLV format	82
17.2.29	Steering Request TLV format	82
17.2.30	Steering BTM Report TLV format	83
17.2.31	Client Association Control Request TLV format	84
17.2.32	Backhaul Steering Request TLV format	84
17.2.33	Backhaul Steering Response TLV format.....	85
17.2.34	Higher Layer Data TLV format	85
17.2.35	Associated STA Traffic Stats TLV format	85
17.2.36	Error Code TLV format.....	86
17.2.37	Channel Scan Reporting Policy TLV format	87
17.2.38	Channel Scan Capabilities TLV format.....	87
17.2.39	Channel Scan Request TLV format	88
17.2.40	Channel Scan Result TLV format	89
17.2.41	Timestamp TLV format	91
17.2.42	CAC Request TLV format	91
17.2.43	CAC Termination TLV format.....	92
17.2.44	CAC Completion Report TLV format.....	93
17.2.45	CAC Status Report TLV format.....	93
17.2.46	CAC Capabilities TLV format	94
17.2.47	Multi-AP Profile TLV format	95
17.2.48	Profile-2 AP Capability TLV format	96
17.2.49	Default 802.1Q Settings TLV format.....	96
17.2.50	Traffic Separation Policy TLV format	96

17.2.51	Profile-2 Error Code TLV format	97
17.2.52	AP Radio Advanced Capabilities TLV format	97
17.2.53	Association Status Notification TLV format.....	97
17.2.54	Source Info TLV format.....	98
17.2.55	Tunneled message type TLV format.....	98
17.2.56	Tunneled TLV format	98
17.2.57	Profile-2 Steering Request TLV format.....	99
17.2.58	Unsuccessful Association Policy TLV format.....	100
17.2.59	Metric Collection Interval TLV format.....	100
17.2.60	Radio Metrics TLV format	101
17.2.61	AP Extended Metrics TLV format.....	101
17.2.62	Associated STA Extended Link Metrics TLV format	102
17.2.63	Status Code TLV format	102
17.2.64	Reason Code TLV format	103
17.2.65	Backhaul STA Radio Capabilities TLV format	103
17.2.66	Backhaul BSS Configuration TLV	103
18	MULTI-AP PROFILES	104
19	TRAFFIC SEPARATION	106
19.1	Traffic Separation in Multi-AP Network	106
19.1.1	Traffic Separation Overview (Informative)	106
19.1.2	Multi-AP Controller Requirements	108
19.1.3	Multi-AP Agent Requirements.....	108
19.2	VLAN Tagging in Multi-AP	110
APPENDIX A	(INFORMATIVE) MISCELLANEOUS	112
A.1	Higher layer protocol field definition (see 16)	112
A.2	Indication of associated 802.11 clients	112
A.3	Implementation Notes (Informative).....	112
A.3.1	Traffic Separation.....	112
A.3.2	Controller implementation for Policy Set Up	112
A.3.3	Fragmentation of IEEE 1905.....	112
A.3.4	Multi-AP Logical Ethernet Interfaces.....	112

List of tables

Table 1.	Definitions	11
Table 2.	Abbreviations and acronyms.....	14
Table 3.	Multi-AP IE format	21
Table 4.	Multi-AP Default 802.1Q Setting subelement	21
Table 5.	Extension of 1905 Media type Table 6-12 in [2]	22
Table 6.	Extension of Authentication Types Table 32 in [5].....	25
Table 7.	Multi-AP Extension subelement	26
Table 8.	Multi-AP Profile subelement.....	27
Table 9.	Message types	54
Table 10.	Message Content by Profile.....	58
Table 11.	SupportedService TLV format.....	67
Table 12.	SearchedService TLV format.....	67
Table 13.	AP Radio Identifier TLV format	67
Table 14.	AP Operational BSS TLV format.....	68
Table 15.	Associated Clients TLV format.....	68
Table 16.	AP Capability TLV format.....	68
Table 17.	AP Radio Basic Capabilities TLV format.....	69
Table 18.	AP HT Capabilities TLV format	69
Table 19.	AP VHT Capabilities TLV format.....	70
Table 20.	AP HE Capabilities TLV format.....	71
Table 21.	Steering Policy TLV format	72
Table 22.	Metric Reporting Policy TLV format	73
Table 23.	Channel Preference TLV format	74
Table 24.	Radio Operation Restriction TLV format	75
Table 25.	Transmit Power Limit TLV format	76
Table 26.	Channel Selection Response TLV format.....	76
Table 27.	Operating Channel Report TLV format	77
Table 28.	Client Info TLV format	77
Table 29.	Client Capability Report TLV format	77
Table 30.	Client Association Event TLV format	78
Table 31.	AP Metric Query TLV format.....	78
Table 32.	AP Metrics TLV format.....	78
Table 33.	STA MAC Address Type TLV format	79
Table 34.	Associated STA Link Metrics TLV format	80
Table 35.	Unassociated STA Link Metrics Query TLV format	80
Table 36.	Unassociated STA Link Metrics Response TLV format.....	81
Table 37.	Beacon Metrics Query TLV format.....	81
Table 38.	Beacon Metrics Response TLV format	82
Table 39.	Steering Request TLV format	82
Table 40.	Steering BTM Report TLV format	83
Table 41.	Client Association Control Request TLV format	84
Table 42.	Backhaul Steering Request TLV format.....	84
Table 43.	Backhaul Steering Response TLV format.....	85
Table 44.	Higher Layer Data TLV format.....	85
Table 45.	Associated STA Traffic Stats TLV.....	85
Table 46.	Error Code TLV format.....	86
Table 47.	Channel Scan Reporting Policy TLV.....	87
Table 48.	Channel Scan Capabilities TLV	88
Table 49.	Channel Scan Request TLV	89
Table 50.	Channel Scan Result TLV.....	89
Table 51.	Timestamp TLV	91
Table 52.	CAC Request TLV format	92
Table 53.	CAC Termination TLV format.....	92
Table 54.	CAC Completion Report TLV format.....	93
Table 55.	CAC Status Report TLV format.....	93
Table 56.	CAC Capabilities TLV format	94

Table 57.	Multi-AP Profile TLV format	95
Table 58.	Profile-2 AP Capability TLV format	96
Table 59.	Default 802.1Q Settings TLV format	96
Table 60.	Traffic Separation Policy TLV format	96
Table 61.	Profile-2 Error Code TLV format	97
Table 62.	AP Radio Advanced Capabilities TLV format	97
Table 63.	Association Status Notification TLV format	98
Table 64.	Source Info TLV format	98
Table 65.	Tunneled message type TLV format	98
Table 66.	Tunneled TLV format	99
Table 67.	Profile-2 Steering Request TLV format	99
Table 68.	Unsuccessful Association Policy TLV format	100
Table 69.	Metric Collection Interval TLV format	100
Table 70.	Radio Metrics TLV format	101
Table 71.	AP Extended Metrics TLV format	101
Table 72.	Associated STA Extended Link Metrics TLV format	102
Table 73.	Status Code TLV format	102
Table 74.	Reason Code TLV format	103
Table 75.	Backhaul STA Radio Capabilities TLV format	103
Table 76.	Backhaul BSS Configuration TLV format	103
Table 77.	Profile Section Applicability	104
Table 78.	Higher layer protocol field definition	112

List of figures

Figure 1.	Multi-AP example deployment 1	16
Figure 2.	Multi-AP example deployment 2	17
Figure 3.	Multi-AP example deployment 3	18
Figure 4.	Onboarding/Configuring BSS	19
Figure 5.	Example Network Configuration with Traffic Separation Enabled	107
Figure 6.	IEEE 802.11 frame with 802.1Q C-TAG	111
Figure 7.	Ethernet frame with 802.1Q C-TAG	111

1 Overview

1.1 Scope

This document is the technical specification for Wi-Fi CERTIFIED EasyMesh™, the Wi-Fi Alliance® certification program for Multi-AP. This specification defines the control protocols between Wi-Fi® access points (APs) as well as the data objects necessary to enable onboarding, provisioning, control and management of multiple APs. This specification also defines the mechanism to route traffic between Wi-Fi access points within the Multi-AP network.

1.2 Purpose

The purpose of this specification is to enable interoperability across Wi-Fi access points (APs) from different vendors in a Wi-Fi network deployment comprising multiple APs.

2 References

- [1] IEEE Computer Society, “IEEE Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” (IEEE Std. 802.11-2016) (<https://standards.ieee.org/findstds/standard/802.11-2016.html>)
- [2] IEEE Std 1905.1™-2013, IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies (<https://standards.ieee.org/findstds/standard/1905.1-2013.html>)
- [3] IEEE Std 802.3™-2015, IEEE Standard for Ethernet (<http://ieeexplore.ieee.org/document/7428776/>)
- [4] TR-181 Device Data Model for TR-069 2016, Issue: 2 Amendment 11 Issue Date: July 2016 (https://www.broadband-forum.org/technical/download/TR-181_Issue-2_Amendment-11.pdf)
- [5] Wi-Fi Simple Configuration Technical Specification (<https://www.wi-fi.org/discover-wi-fi/specifications>)
- [6] ISO 3166-1, “Codes for the representation of names of countries and their subdivisions—Part 1: Country codes” (<https://www.iso.org/standard/63545.html>)
- [7] IEEE 802.1Q-2018 - IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks, (https://standards.ieee.org/standard/802_1Q-2018.html)
- [8] Wi-Fi Agile Multiband Specification v1.2 (<https://www.wi-fi.org/file/wi-fi-agile-multiband-specification>)
- [9] Optimized Connectivity Experience Technical Specification v1.0 (<https://www.wi-fi.org/file/optimized-connectivity-experience-technical-specification-v10>)
- [10] Data Elements Technical Specification v1.0 (<https://www.wi-fi.org/file/data-elements-specification-package>)
- [11] IEEE 1905.1a-2014, IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies Amendment 1: Support of New MAC/PHYs and Enhancements (https://standards.ieee.org/standard/1905_1a-2014.html)
- [12] Wi-Fi Multimedia Technical Specification (with WMM-Power Save and WMM-Admission Control) Version 1.2.0 (<https://www.wi-fi.org/file/wmm-specification-v12>)

3 Definitions and acronyms

3.1.1 Shall/should/may/might word usage

The words "shall", "should", and "may" are used intentionally throughout this document to identify the normative text for the Multi-AP program. The words "can" and "might" shall not be used to define normative requirements.

The word *shall* indicates a mandatory requirement. All mandatory requirements must be implemented to assure interoperability with other Multi-AP products.

The word *should* denotes a recommended approach or action.

The word *may* indicates a permitted approach or action with no implied preference.

The words *might* and *can* indicate a possibility or suggestion.

3.1.2 Conventions

The ordering of bits and bytes in the fields within TLVs, information elements and attributes shall follow the conventions in [2] unless otherwise stated.

The word *ignored* shall be used to describe bits, bytes, fields or parameters whose values are not verified by the recipient.

The word *reserved* shall be used to describe objects (bits, bytes, or fields or their assigned values) whose usage and interpretation will be defined in the future by this specification or by other technical specifications/bulletins. A reserved object shall be set to zero unless otherwise stated. The recipient of a reserved object shall ignore its value unless that object becomes defined at a later date. The sender of an object defined by this technical specification shall not use a reserved code value.

3.1.3 Definitions

The definitions in Table 1 are applicable to this specification.

Table 1. Definitions

Term	Definition
802.1Q C-TAG	A Customer Virtual Local Area Network [C-VLAN] tag as specified in section 3.58 of [7].
802.1Q C-VID	A Customer Virtual Local Area Network [C-VLAN] identifier as specified in section 3.57 of [7].
802.1Q VLAN Tag	Any VLAN tag specified in [7], including C-VLAN and S-VLAN tags.
Air Time	The time-frequency spectral resources, normalized to the operating bandwidth of the BSS. Therefore, if the predicted bandwidth of backhaul transmissions is less than the BSS operating bandwidth (e.g. due to dynamic bandwidth adjustment and/or HE OFDMA allocation), this is factored in to the percentage of air time indicated.
Available Channel	A channel that the Multi-AP Agent can actively use immediately without needing to perform a CAC.
backhaul link	A Wi-Fi link or wired Logical Ethernet Link between two Multi-AP devices in a Multi-AP network.
backhaul SSID	A Wi-Fi SSID used for a Wi-Fi backhaul link that is either the same or different from the fronthaul SSID.
backhaul STA	A STA on a Multi-AP device with a Multi-AP Agent that provides Wi-Fi connectivity with other Wi-Fi access points over the backhaul link.
CAC Completion Action	The action a Multi-AP Agent takes upon completing a CAC. CAC completion actions include remaining on the channel where the CAC was performed and continuing to monitor for radar, or returning to the previous state before the CAC was started.

Term	Definition
Channel Availability Check (CAC)	Period of time during which a radio in a Multi-AP Agent monitors for radar, without sending or receiving traffic on the channel being monitored for radar.
Continuous CAC	A method of performing a Channel Availability Check (CAC) in which one of the radios that would normally be used for communication ceases normal operation and listens continuously on the channel being CAC'ed. Using this method, the radio is not available for any other purpose while the CAC is being performed.
Continuous CAC with dedicated radio	A method of performing a Channel Availability Check (CAC) in which the device performing the CAC employs an additional radio, that has not been in use for communication, to perform the CAC. The additional radio allows the CAC to be performed while the device continues to operate with the equivalent capabilities as when it is not performing a CAC.
Controller DFS Channel Clear Indication	An indication provided by the Multi-AP Controller to a Multi-AP Agent as part of a Channel Preference TLV within a Channel Selection Request message that indicates that the Multi-AP Agent may begin operating on that channel without having to perform a CAC.
Egress Packet	Any packet leaving a Multi-AP Profile-2 Network Segment via an interface of a Multi-AP Agent that implements Profile-2, including all packets sent on the Wi-Fi fronthaul, Profile-1 Wi-Fi backhaul or any packet sent on a Multi-AP Logical Ethernet Interface that are being carried over the Primary VLAN.
fronthaul AP	An access point (AP) of a Multi-AP device that provides Wi-Fi connectivity to client stations (STAs) and/or backhaul STAs.
Independent Channel Scan	A channel scan initiated by the Multi-AP Agent performing the scan (rather than by the Multi-AP Controller).
Inoperable channel	A channel that a device is temporarily not able to operate on due to reasons such as regulatory restrictions or radio environment.
In-Service Monitoring	Period of time during which a radio in a Multi-AP Agent monitors for radar while transmitting and receiving traffic on the channel being monitored.
Ingress Packet	Any packet generated locally by a Multi-AP Agent that implements Profile-2 or any packet entering a Multi-AP Profile-2 Network Segment via an interface of a Multi-AP Agent that implements Profile-2, including any packet received on, Wi-Fi fronthaul or Profile-1 Wi-Fi backhaul or any packet received on a Multi-AP Logical Ethernet Interface that is not tagged as belonging to a Secondary VLAN.
Logical Ethernet Interface	An interface onto a Logical Ethernet Link.
Logical Ethernet Link	A wired connection that may be Ethernet, Multimedia over Coax Alliance (MoCA), power line communication (PLC) or equivalent.
MIMO Dimension reduced CAC	A method of performing a Channel Availability Check (CAC) in which the device performing the CAC employs one receiving chain from one of the radios to perform the CAC. Using this method, the Rx MIMO capability of the radio performing the CAC is reduced by one while the CAC is being performed.
Multi-AP Agent	A Multi-AP compliant logical entity that executes AP control functions and provides Multi-AP specific control information.
Multi-AP Controller	A Multi-AP compliant logical entity that implements logic for controlling the operation of the Multi-AP network.
Multi-AP device	A Multi-AP physical entity that may contain a Multi-AP Controller only, a Multi-AP Agent only or both Multi-AP Controller and Multi-AP Agent.
Multi-AP Logical Ethernet Interface	A Logical Ethernet Interface that connects Multi-AP devices.
Multi-AP network	A Wi-Fi network deployment comprising of one or more Multi-AP devices.
Multi-AP Profile-2 Network Segment	A set of Multi-AP Agents that implements Profile-2 that are connected to each other by a set of Wi-Fi or Logical Ethernet Links where those links do not pass through a Multi-AP Agent that implements Profile-1 or a device that discards 802.1Q VLAN tags. (See section 8.1 of [2])

Term	Definition
multiple virtual radio operation	Time slicing operation of the physical radio between multiple virtual radios, each operating on a different band or channel.
Non-Occupancy Channels	Channels that have had radar detected on them, and cannot be occupied until the non-Occupancy Duration has expired.
Non-Occupancy Duration	After detection of radar, regulatory domains require that the channel not be used for a period of time. The amount of time remaining (in seconds) until the channel can be used is the Non-Occupancy Duration. Non-occupancy periods are the result of detecting radar during a CAC, while monitoring following the termination or end of a CAC, or while performing in-service monitoring.
Non-operable channel	A channel that a device is permanently not capable of operating on.
Primary Network	The network that a user configures for their own use, covering both Logical Ethernet and Wi-Fi interfaces, and all of the traffic carried onto this network.
Primary VLAN	A unique VLAN that is assigned to the Primary Network traffic.
Requested Channel Scan	A channel scan performed in response to a request from a Multi-AP Controller.
Secondary VLAN	Any VLAN configured by the Multi-AP Controller that implements Profile-2 that is not the Primary VLAN.
Self-Triggered CAC	A CAC started by a Multi-AP Agent of its own volition. These may be performed for a number of reasons, for example if the Multi-AP Agent believes a CAC is required before operating on a channel that it has been requested to operate on.
Simultaneous CAC Radios	The radios in a Multi-AP Agent that are able to perform a CAC simultaneously. For example, if a Multi-AP Agent can only perform one CAC check at a time, then it would have one CAC Radio. If it is able to perform CAC on two channels simultaneously, then it has two Simultaneous CAC Radios.
Steering Mandate mechanism	A mechanism to mandate a Multi-AP Agent to attempt steering of one or more associated STAs.
Steering Opportunity mechanism	A mechanism to provide a time window for a Multi-AP Agent to steer one or more associated STAs.
Successful CAC	A Channel Availability Check (CAC) that proceeds to completion of the required CAC time without detecting radar. Operation in the channel on which the CAC was performed could commence following a Successful CAC.
Time Sliced CAC	A method of performing a Channel Availability Check (CAC) in which one of the radios that normally is used for communications spends a fraction of the time performing the CAC, and the remainder of the time operating normally for communication. Using this method, the data throughput that can be sustained by the radio is reduced roughly by the percentage of time it spends performing the CAC.
Traffic Separation Policy	A group of traffic separation rules that are set in the Multi-AP Controller.
Triggered CAC	A CAC begun by the Multi-AP Controller via a CAC Request message.
Unsuccessful CAC	A CAC that is not a Successful CAC. Unsuccessful CACs can be due to detecting radar, or errors that prevent monitoring the channel for the required CAC time.
Wi-Fi Backhaul	A Wi-Fi link between two Multi-AP devices in a Multi-AP network.
Wi-Fi Fronthaul	A Wi-Fi link between a Multi-AP Agent and its associated non-backhaul STA client stations (STAs).

3.1.4 Abbreviations and acronyms

Table 2 defines the acronyms used throughout this document. Some acronyms are commonly used in publications and standards defining the operation of wireless local area networks, while others have been generated by Wi-Fi Alliance.

Table 2. Abbreviations and acronyms

Acronyms	Definition
1905	IEEE Std 1905.1™-2013, IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies
AC	Access category
AL	Abstraction layer
BSS	Basic service set
BTM	BSS transition management
CAC	Channel availability check
CMDU	Control message data unit
DFS	Dynamic frequency selection
DL	Downlink
EIRP	Effective isotropic radiated power
EUI	Extended unique identifier
GI	Guard interval
GTK	Group temporal key
HE OFDMA	High efficiency orthogonal frequency-division multiplexing
HLE	Higher layer entity
HT	High throughput
IE	Information element
MID	Message identifier
MU	Multi-user
OFDMA	Orthogonal frequency-division multiplexing
PBC	Push-button configuration
PCP	Priority Code Point
PPDU	Physical layer protocol data unit
RCPI	Received channel power indicator
RSSI	Received signal strength indicator
SU	Single user
TBTT	Target beacon transmission time
TU	Time units
UL MU-MIMO	Uplink multi-user multiple input multiple output
VID	VLAN Identifier
VLAN	Virtual Local Area Network
WPS	Wi-Fi Protected Setup™

4 Architecture

4.1 Multi-AP architecture

A Multi-AP network consists of two types of logical entities:

- One Multi-AP Controller and
- One or more Multi-AP Agents

A Multi-AP Controller is a logical entity in a Multi-AP network that implements logic for controlling the fronthaul APs and backhaul links in the Multi-AP network. A single Multi-AP Controller is supported for a given Multi-AP network. A Multi-AP Controller receives measurements and capability data for fronthaul APs, clients and backhaul links from the Multi-AP Agents and triggers AP control related commands and operations on the Multi-AP Agents. A Multi-AP Controller also provides onboarding functionality to onboard and provision Multi-AP devices onto the Multi-AP network.

A Multi-AP Agent is a logical entity that executes the commands received from the Multi-AP Controller, and reports measurements and capabilities data for fronthaul APs, clients and backhaul links to a Multi-AP Controller and/or to other Multi-AP Agents. A Multi-AP Agent interfaces with Wi-Fi sub-systems for fronthaul APs and backhaul STA on the Multi-AP device to get measurements and capabilities data, apply configuration changes and execute AP control functions.

A logical Multi-AP control interface is defined between Multi-AP devices over which configuration and control functions for fronthaul APs and backhaul links are executed. A Multi-AP control interface exists between the Multi-AP Controller and Multi-AP Agents. A Multi-AP interface may exist between two Multi-AP Agents.

A Multi-AP device may contain a Multi-AP Controller only, a Multi-AP Agent only, or both Multi-AP Controller and Multi-AP Agent. Two Multi-AP devices with Multi-AP Agents connect to each other over a backhaul link, which could be either a Wi-Fi link or a wired Logical Ethernet Link. A single active backhaul link is allowed between any two Multi-AP devices at any given time.

A Multi-AP device with a Multi-AP Agent includes fronthaul AP(s) for client STAs and/or a backhaul STA to associate with for Wi-Fi backhaul connectivity. In cases where a Wi-Fi backhaul link is supported, a Multi-AP device with a Multi-AP Agent also includes a backhaul STA to enable Wi-Fi backhaul link with another upstream fronthaul AP (see Figure 2).

Multi-AP devices with Multi-AP Agent functionality are connected to each other in a tree topology over one or more hops within a Multi-AP network. The tree topology ensures that a single backhaul path (over one or more hops) is established between any two Multi-AP devices in a Multi-AP network.

The Multi-AP features defined in this specification are grouped into "Profiles". A Multi-AP device is said to implement a given Profile when it implements all the features mandated by such profile, as detailed in Table 77 in section 18. Profiles are numbered and referred to as "Profile-X", where X is an integer greater than or equal to 1.

4.1.1 Multi-AP example deployment

Figure 1 shows an example of a Multi-AP deployment with two Multi-AP devices.

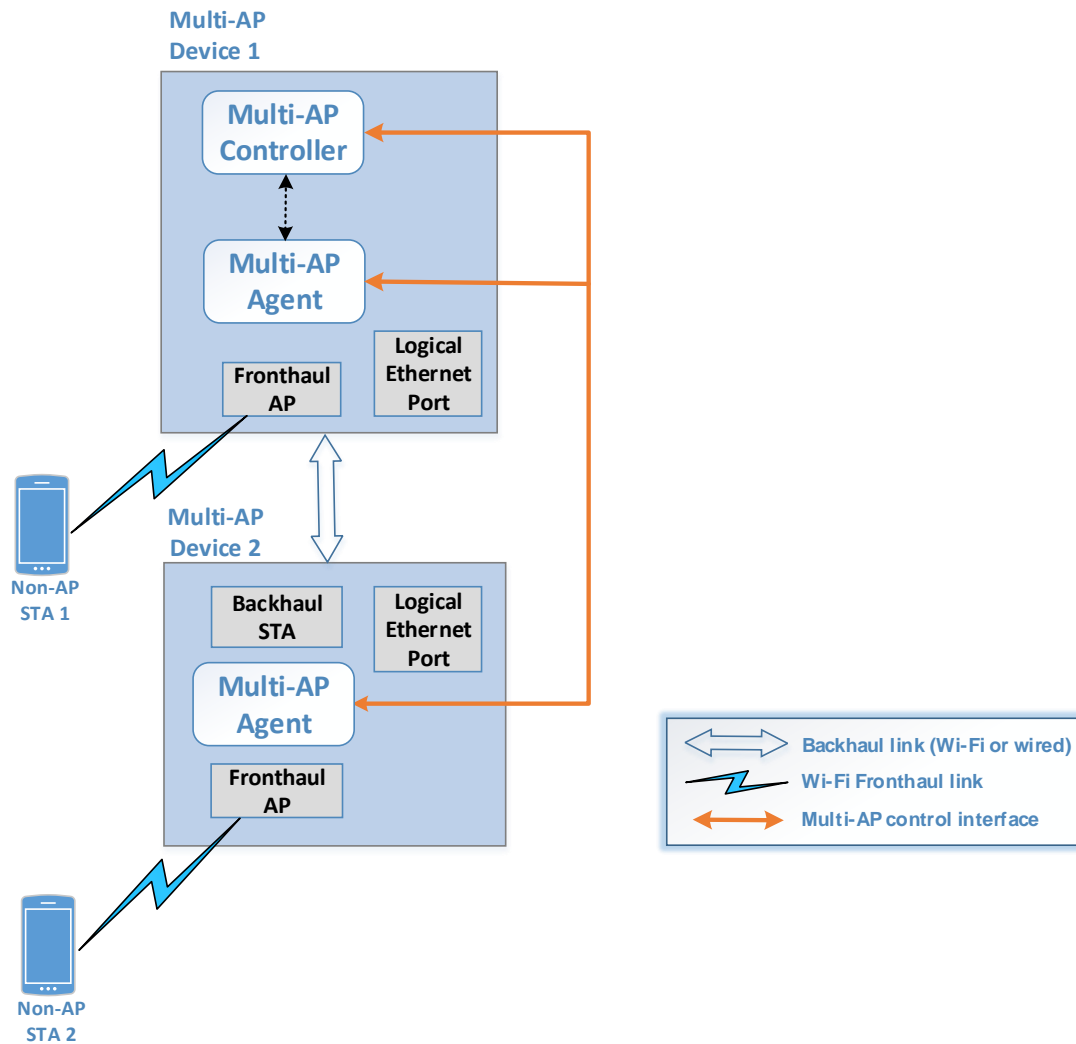


Figure 1. Multi-AP example deployment 1

Figure 2 shows another example of a Multi-AP deployment with four Multi-AP devices organized in a tree topology with a maximum of two hops between the Multi-AP devices.

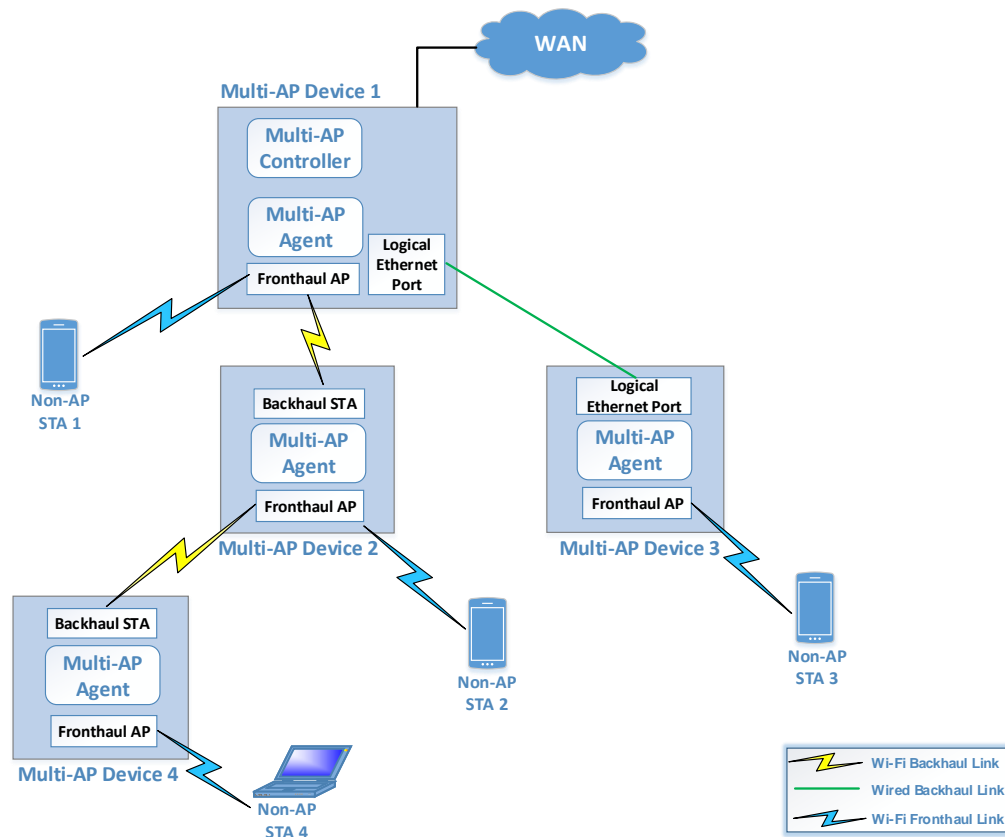


Figure 2. Multi-AP example deployment 2

Figure 3 shows another example of a Multi-AP deployment with four Multi-AP devices and with the Multi-AP Controller entity deployed on a separate Multi-AP device.

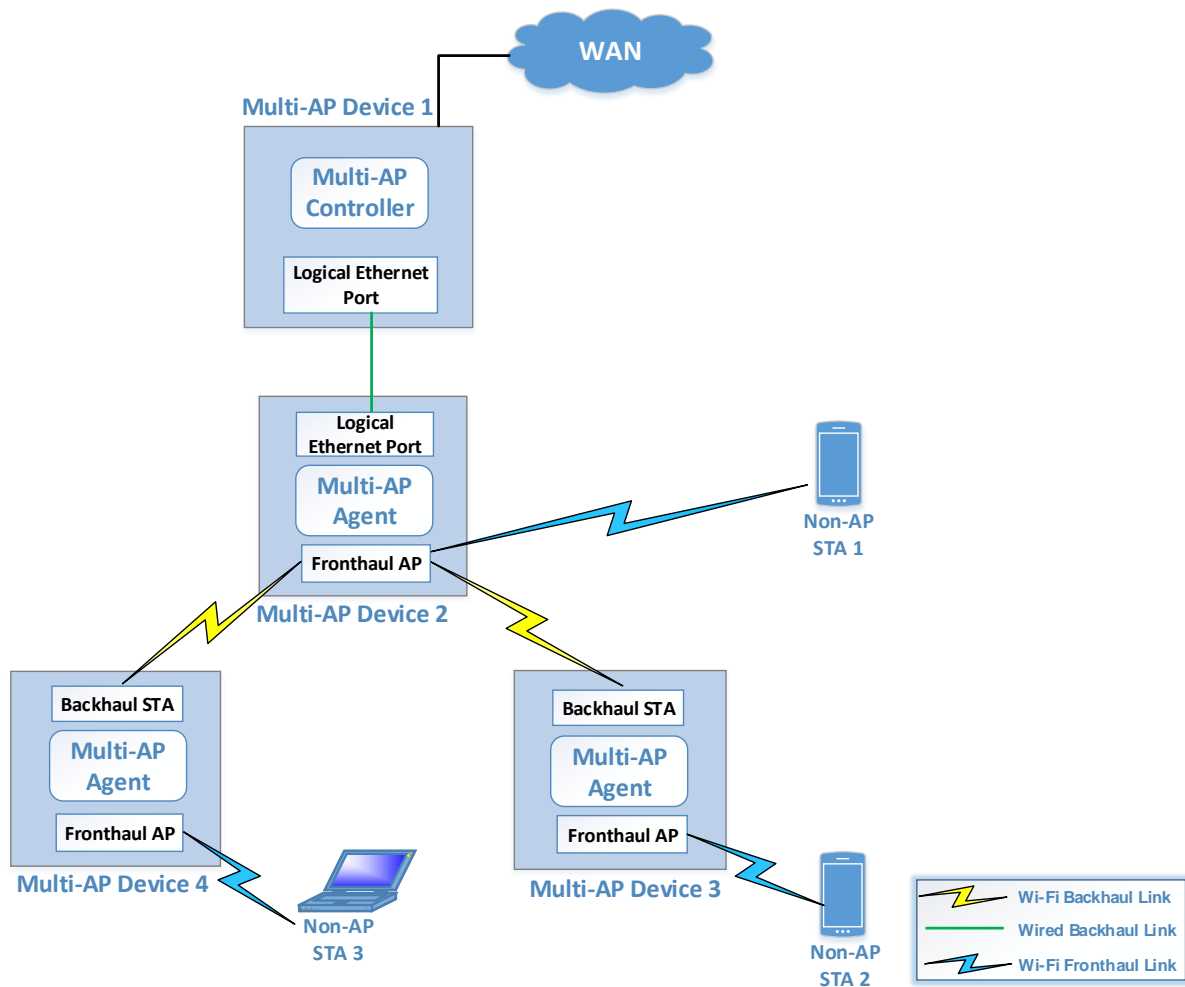


Figure 3. Multi-AP example deployment 3

5 Multi-AP onboarding

Onboarding is the process by which a Multi-AP Agent gains layer-2 connectivity onto a Multi-AP network through Wi-Fi or wired connectivity. This specification defines one mandatory method (see section 5.2) by which a Multi-AP device that includes a Multi-AP Agent and backhaul STA can onboard to a Multi-AP network. Note that a backhaul STA might be provisioned with backhaul credentials using out of band method(s). Once layer-2 connectivity is established by any method, the Multi-AP Agent commences discovery of the Multi-AP Controller per section 6.1.

5.1 1905 Push Button Configuration method

A Multi-AP Agent with a backhaul STA shall support the 1905 Push Button Configuration (1905 PBC) method of [2] with the extensions per section 5.2.

5.2 PBC Backhaul STA onboarding procedure

An enrollee backhaul STA uses an extension to the PBC onboarding method, as defined in section 5.1, to indicate to an existing Multi-AP Agent that it is a backhaul STA (see Figure 4). In Figure 4, it is assumed that a Multi-AP Controller previously configured the existing Multi-AP Agent with the supported BSS backhaul STA connections using an extension to the 1905 AP-Autoconfiguration procedures per 7.1 (see Figure 4).

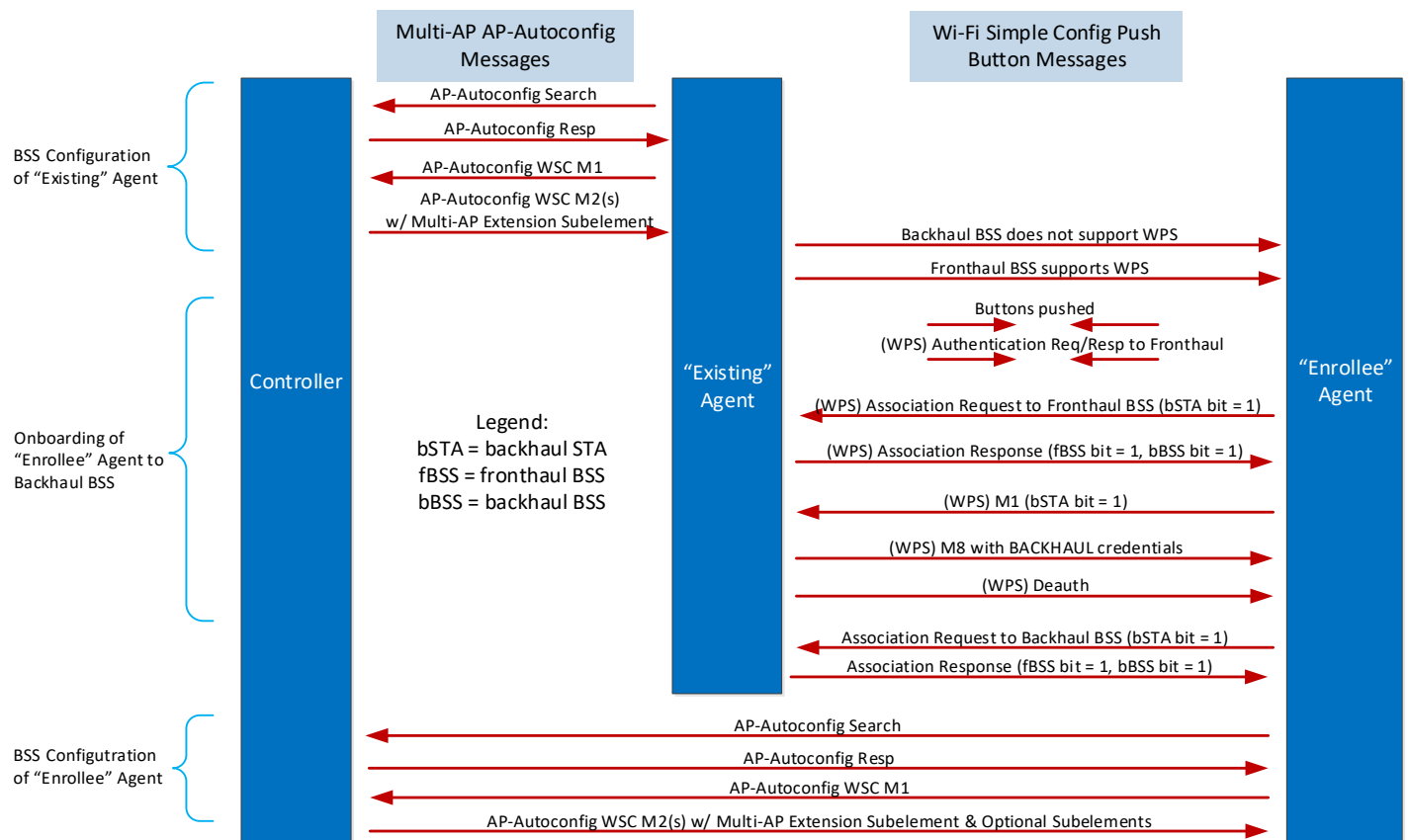


Figure 4. Onboarding/Configuring BSS

BSS Configuration

If a Multi-AP Agent operates a BSS that has been configured to support the Backhaul BSS role but has not been configured to support the Fronthaul BSS role, the Multi-AP Agent shall not advertise Wi-Fi Protected Setup (WPS) support on that BSS.

If a Multi-AP Agent operates one or more BSSs that has been configured to support Fronthaul BSS, the Multi-AP Agent shall advertise WPS support on at least one of those BSSs.

If a backhaul STA sends a (Re-)Association Request frame from its backhaul STA interface, it shall include in the frame a Multi-AP IE (see Table 3) containing a Multi-AP Extension subelement where bit 7 of the subelement value is set to one to indicate it is a backhaul STA.

If a Multi-AP Agent operates a BSS that has been configured to support Fronthaul BSS, the Multi-AP Agent shall include a Multi-AP IE containing a Multi-AP Extension subelement with bit 5 of the subelement value set to one to indicate Fronthaul BSS in all (Re-)Association Response frames sent from that BSS to STAs identifying themselves as backhaul STAs.

If a Multi-AP Agent operates a BSS that has been configured to support Backhaul BSS, the Multi-AP Agent shall include a Multi-AP IE containing a Multi-AP Extension subelement with bit 6 of the subelement value set to one to indicate Backhaul BSS in all (Re-)Association Response frames sent from that BSS to STAs identifying themselves as backhaul STAs. If a Multi-AP Agent operates a backhaul BSS configured with Profile-1 bSTA Disallowed the Multi-AP Agent shall set bit 3 of the Multi-AP Extension subelement to one. If a Multi-AP Agent operates a BSS configured with Profile-2 bSTA Disallowed, the Multi-AP Agent shall set bit 2 of the Multi-AP Extension subelement to one.

If a Multi-AP Agent that implements Profile-2 sends a Multi-AP IE in a (Re)Association Request or Response frame, it shall include a Multi-AP Profile subelement with the Multi-AP Profile field set to 0x02.

If a Multi-AP Agent that implements Profile-2 sends a Multi-AP IE in a (Re)Association Response frame of a Backhaul BSS, and the most recently received Traffic Separation Policy has the number of SSIDs field set to a value different than zero, it shall include a Multi-AP Default 802.1Q Setting subelement (as defined in Table 4) with the latest configured Primary VLAN ID. If a Multi-AP Agent that implements Profile-2 sends a Multi-AP IE in a (Re)Association Response frame of a Backhaul BSS, and it considers the Primary VLAN ID not configured, it shall not include a Multi-AP Default 802.1Q Setting subelement.

Backhaul STA Configuration

If a backhaul STA sends an M1 message (see [5]) from its backhaul STA interface during a WPS exchange, it shall include a Multi-AP Extension subelement in the M1 message as part of the Wi-Fi Alliance Vendor Extension attribute with bit 7 of the subelement value set to one to indicate it is a backhaul STA.

If a Multi-AP Agent receives an M1 message with bit 7 of the Multi-AP Extension subelement, as part of the Wi-Fi Alliance Vendor Extension attribute set to one from a STA during the WPS procedure, the Multi-AP Agent shall configure the backhaul STA with credentials (i.e. SSID and passphrase) pertaining to the backhaul SSID.

If a Multi-AP Agent's backhaul STA uses WPS to be configured with network credentials by another Multi-AP Agent and the backhaul STA has been deauthenticated by the AP at the end of the WPS procedure, the Multi-AP Agent's backhaul STA shall associate to the backhaul SSID using the configured credentials.

If a Multi-AP Agent backhaul STA supports SAE and the configured credentials comprise a WPA2-Personal passphrase and the Multi-AP Agent discovers an AP that is advertising the backhaul SSID and an SAE AKM, the Multi-AP Agent shall attempt SAE authentication with the AP (instead of WPA2-Personal) using the configured passphrase.

If the Backhaul STA of a Multi-AP Agent that implements Profile-2 has successfully associated with a Backhaul BSS whose latest (Re)Association Response frame contains a Multi-AP Default 802.1Q Setting subelement (Table 4) in the Multi-AP IE with a Primary VLAN ID that differs from the one in use on the newly-associated Agent, or no Primary VLAN ID is configured on the newly-associated Agent, then the newly-associated Agent shall configure the Primary VLAN ID to the one indicated in the Multi-AP Default 802.1Q Setting subelement and send any 1905.1 management frames as defined in section 19.1.3. If the Backhaul STA of a Multi-AP Agent implements Profile-2 has successfully associated with a Backhaul BSS whose latest (Re)Association Response frame does not contain a Multi-AP Default 802.1Q Setting subelement (Table 4) in the Multi-AP IE and the newly-associated Agent has a Primary VLAN ID configured, the newly-

associated Multi-AP Agent shall consider the Primary VLAN ID not configured and send any 1905.1 management frames as defined in section 19.1.3.

Table 3. Multi-AP IE format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 vendor specific information element.
Length	1	Variable	Length of the following fields in the IE in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to 9.4.1.32 of [1])
OUI Type	1	0x1B	Wi-Fi Alliance specific OUI Type identifying the type of the Multi-AP IE.
Subelement related fields	3	Variable	Multi-AP Extension subelement per Table 7.
	3	Variable	Multi-AP Profile subelement per Table 8.
	4	Variable	Multi-AP Default 802.1Q Setting subelement per Table 4.

Table 4. Multi-AP Default 802.1Q Setting subelement format

Field	Length	Value	Description
Subelement ID	1 octet	0x08	Multi-AP Default 802.1Q Setting subelement identifier.
Subelement Length	1 octet	0x02	Number of Bytes in the subelement value.
Subelement Value	2 octets	Variable	Primary VLAN ID. This subfield shall be transmitted in little endian byte order.

6 Multi-AP discovery

A discovery scheme is used to discover Multi-AP Controller and Multi-AP Agents in a Multi-AP network that is based on an extension of the discovery functionality defined in [2].

Note: A Multi-AP Agent supporting [11] might use the Generic PHY query/response procedure to discover Generic Phy non-Wi-Fi interfaces.

Additional Wi-Fi Media type (intfType) value(s) to 1905 Media type Table 6-12 (see [2]):

Table 5. Extension of 1905 Media type Table 6-12 in [2]

Media Type (intfType)		Description	Media-specific information (n octets)
Bits 15 to 8	Bits 7 to 0		
1	8	Wi-Fi 6	n=0

6.1 Multi-AP controller discovery

A Multi-AP network shall be configured with a single Controller for the Multi-AP network.

If a Multi-AP device can be configured as a Controller through an out-of-band mechanism (e.g. through UI or Service Provider configuration), the configuration shall be stored in non-volatile memory and the configuration shall be used after restart of the device.

Note: If a Multi-AP device that implements Profile-2 implements an Agent and a Controller, then it might provide an out-of-band mechanism by which a user can disable the Controller function if they wish to onboard this as a Multi-AP Agent to an existing Multi-AP network. For example, this could be implemented directly by presenting the user with a Controller on/off selection or indirectly by presenting the user with a choice such as “Is this a new network or an existing network?”.

Note: If a Multi-AP device that implements Profile-2 implements an Agent and a Controller and the Agent initiates onboarding onto an existing Multi-AP network (see section 5) using a Wi-Fi interface, it might disable its Controller functionality and store this configuration in its non-volatile memory.

Note: If a Multi-AP device that implements Profile-2 implements an Agent and a Controller and a non-Wi-Fi interface transitions to the PWR_ON state, it might send a 1905 AP-Autoconfiguration Search message (see section 6.3.7 of [2]) on that interface. If the Multi-AP device receives a 1905 AP-Autoconfiguration Response message (see section 6.3.8 of [2]) on a non-Wi-Fi interface from a Controller that is not its Controller, it might disable its Controller functionality and store this configuration in its non-volatile memory.

Note: A Multi-AP Controller might send a 1905 AP-Autoconfiguration Search message to discover the possible presence of another Multi-AP Controller. If the Multi-AP Controller receives a 1905 AP-Autoconfiguration Response message, it might send a notification to the upper layers.

This specification extends the 1905 AP-Autoconfiguration search/response procedure (see section 10 of [2]) to allow discovery of a Multi-AP Controller. The Multi-AP Controller shall be co-located with the 1905 Registrar functionality in the same physical device.

To discover a Multi-AP Controller, a Multi-AP Agent sends a 1905 AP-Autoconfiguration Search message (see section 6.3.7 of [2]). The Multi-AP Controller responds with a 1905 AP-Autoconfiguration Response message (see section 6.3.8 of [2]). A Multi-AP Agent that implements Profile-2 shall include one Multi-AP Profile TLV (see section 17.2.47) in the 1905 AP-Autoconfiguration Search message with the Multi-AP Profile field set to Multi-AP Profile-2.

A Multi-AP Agent shall indicate Registrar in the SearchedRole TLV in the 1905 AP-Autoconfiguration Search message. A Multi-AP Agent shall include SupportedService TLV and SearchedService TLV in the 1905 AP-Autoconfiguration Search message per section 17.1.1. A Multi-AP Agent shall indicate Multi-AP Agent in the SupportedService TLV in the 1905 AP-Autoconfiguration Search message. A Multi-AP Agent shall indicate Multi-AP Controller in the SearchedService TLV in the 1905 AP-Autoconfiguration Search message.

If a Multi-AP Controller receives a 1905 AP-Autoconfiguration Search message with SearchedRole set to Registrar and SearchedService set to Multi-AP Controller, it shall include SupportedService TLV in the 1905 AP-Autoconfiguration Response message per section 17.1.2. A Multi-AP Controller shall indicate Registrar in the SupportedRole TLV in the 1905 AP-Autoconfiguration Response message. A Multi-AP Controller shall indicate Multi-AP Controller in the SupportedService TLV in the 1905 AP-Autoconfiguration Response message. A Multi-AP Controller that implements Profile-2 shall include one Multi-AP Profile TLV in the 1905 AP-Autoconfiguration Response message with the Multi-AP Profile field set to Multi-AP Profile-2.

6.2 Multi-AP service discovery

This specification extends the 1905 Topology query/response procedure (see section 8 of [2]) to allow discovery of Multi-AP specific capabilities provided by Multi-AP devices.

To discover the Multi-AP specific capabilities of a Multi-AP device, a Multi-AP Controller or a Multi-AP Agent sends a 1905 Topology Query message to the Multi-AP device (per section 8 of [2]). The Multi-AP device responds with a 1905 Topology Response message (per section 17.1.4).

A Multi-AP Controller or a Multi-AP Agent shall include a SupportedService TLV in the 1905 Topology Response message. If the Multi-AP device includes a Multi-AP Agent, the Multi-AP Agent shall indicate Multi-AP Agent in the SupportedService TLV in the 1905 Topology Response message. If the Multi-AP device includes a Multi-AP Controller, the Multi-AP Controller shall indicate Multi-AP Controller in the SupportedService TLV in the 1905 Topology Response message.

If a Multi-AP device that implements Profile-2 sends a Topology Query message, it shall include one Multi-AP Profile TLV in the 1905 Topology Query message with the Multi-AP Profile field set to Multi-AP Profile-2.

If a Multi-AP Agent sends a Topology Response message and there is at least one 802.11 client directly associated with any of the BSS(s) that is operated by the Multi-AP Agent, the Multi-AP Agent shall include an Associated Clients TLV in the message per section 17.1.4 to indicate all the 802.11 clients that are directly associated with each of the BSS(s) that is operated by the Multi-AP Agent. See A.2 for further explanation.

If a Multi-AP device that implements Profile-2 sends a Topology Response message, it shall include one Multi-AP Profile TLV in the 1905 Topology Response message with the Multi-AP Profile field set to Multi-AP Profile-2.

6.3 Client association and disassociation notification

This specification extends the 1905 Topology Notification message to allow other Multi-AP Agents to learn of client (re)association and disassociation events quickly.

If a Wi-Fi client joins or leaves a BSS on a Multi-AP device, the Multi-AP Agent shall include a Client Association Event TLV in the 1905 Topology Notification message per section 17.1.5.

If a Multi-AP Agent that implements Profile-2 sends a 1905 Topology Notification message including a Client Association Event TLV with the Association Event bit set to zero (client disassociation), the Multi-AP Agent shall also send to the Multi-AP Controller a Client Disassociation Stats message including one STA MAC Address TLV identifying the station that has disassociated, one Reason Code TLV with the Reason Code set to indicate the reason for the disassociation or deauthentication as defined in Table 9-45 of [1] and one Associated STA Traffic Stats TLV indicating the final traffic stats of that client session.

If a Multi-AP Agent that implements Profile-2 most recently received Multi-AP Policy Config Request contains an Unsuccessful Association Policy TLV with the Report Unsuccessful Associations bit set to one, and if the Multi-AP Agent has sent fewer than the maximum number of Failed Connection messages (as specified in the Maximum Reporting Rate element of the Unsuccessful Association Policy TLV) in the preceding minute, and the Multi-AP Agent detects that Wi-Fi client has made a failed attempt to connect to any BSS operated by the Multi-AP Agent, the Multi-AP Agent shall send to the Multi-AP Controller a Failed Connection message including a STA MAC Address TLV identifying the client that has attempted to connect and a Status Code TLV with the Status Code set to a non-zero value that indicates the reason for association or authentication failure as defined in Table 9-46 of [1], or a Status Code TLV with the Status Code set to zero and a Reason Code TLV with the Reason Code indicating the reason the STA was disassociated or deauthenticated as defined in Table 9-45 of [1].

Note: A STA does not send a Disassociation or Deauthentication frame to the source BSS when roaming using the 802.11 Reassociation procedure. If a STA roams away from a BSS for which it has negotiated Protected Management Frames with the AP, and subsequently attempts to (re)associate to that same BSS while the AP maintains associated state for the STA from the original association (i.e. if the AP has not realized that the STA left the BSS), the AP will initiate a security procedure per IEEE 802.11 standard intended to protect the original association from unauthorized teardown. This procedure involves rejection of the subsequent (re)association request for a timeout period, which can result in significant outage for the STA. To avoid such outage, it is necessary for a Multi-AP Agent to internally synchronize association state between BSSs it is operating, and also to determine when an associated STA has roamed to a BSS of another Multi-AP Agent. For the latter, 1905 Topology Notification messages received from other Multi-AP Agents might be used. A possible race condition might occur when the STA roams away and then rapidly attempts to (re)associate back to the source BSS before the message indicating the initial roam has been received.

7 Multi-AP configuration

7.1 AP configuration

This specification extends the 1905 AP-Autoconfiguration procedure to enable a Multi-AP Controller to configure 802.11 interfaces (i.e. BSS) on each of the radio(s) of a Multi-AP Agent. A Multi-AP Agent treats each of its unconfigured radio(s) as an “unconfigured IEEE 802.11 interface” in section 10.1 of [2]. A Multi-AP Controller configures Traffic Separation policies using AP-Autoconfiguration WSC messages and / or Multi-AP AP Policy Config Request messages (see Section 19.1.2).

This specification extends the Authentication Types in Table 32 of [5] by defining a new value 0x0040 for SAE.

Table 6. Extension of Authentication Types Table 32 in [5]

Value	Authentication Types	Notes
0x0040	SAE	

To initiate (re)configuration of a radio, a Multi-AP Agent shall send an AP-Autoconfiguration WSC message per section 17.1.3. A Multi-AP Agent shall send a separate AP-Autoconfiguration WSC message per section 17.1.3 for each of its radio(s). The Multi-AP Agent shall indicate the radio of the 802.11 configuration with a Radio Unique Identifier in the AP Radio Basic Capabilities TLV (see section 17.2.7). The Multi-AP Agent shall set the MAC Address attribute in M1 in the AP-Autoconfiguration WSC message to the 1905 AL MAC address of the Multi-AP device. The Multi-AP Agent shall set the Authentication Type Flags attribute in M1 in the AP-Autoconfiguration WSC message to one of the values allowed in [5] or to 0x0040 (indicating SAE) or to any valid combination, depending on the radio's supported AKMs from Table 9-133 of [1]. If a Multi-AP Agent that implements Profile-2 sends an AP-Autoconfiguration WSC message, it shall include one Profile-2 AP Capability TLV and one AP Radio Advanced Capabilities TLV.

If a Multi-AP Controller receives a WSC TLV containing an M1, then it shall respond within one second with either 1) one or more M2s for each BSS to be configured on the radio identified in the AP Radio Identifier TLV or 2) one M2 with bit 4 (Tear down bit) set to one in the Multi-AP Extension subelement to indicate that zero BSS are to be configured on the radio identified in the AP Radio Identifier TLV per section 17.1.3.

A Multi-AP Controller shall include one WSC TLV containing an M2 (see [5]) for each BSS to be configured on the radio identified in the AP Radio Identifier TLV in an AP-Autoconfiguration WSC message per section 17.1.3. The N2 nonce specified in each M2 shall be unique. A Multi-AP Controller shall set the Authentication Type attribute in M2 to one of the values allowed in [5] or to 0x0040 (indicating SAE) or to any valid combination, as per the Multi-AP Agent declaration in M1's Authentication Types Flags.

A Multi-AP Controller indicates whether or not a BSS is to support Multi-AP backhaul connections and/or fronthaul connections in the Multi-AP Extension subelement listed in Table 7 as part of AP-Autoconfiguration WSC message illustrated in Figure 4. If a Multi-AP Controller sends an M2 indicating Fronthaul BSS, it shall not set the Authentication Type attribute in that M2 to 0x0040 (SAE only).

The Multi-AP Controller shall not configure SAE-only mode on fronthaul BSSs. However, if the Multi-AP Agent indicates support for SAE in the M1, the Controller might configure a fronthaul BSS to 0x0060 (PSK+SAE), aka WPA3 Transition Mode.

The Multi-AP Extension subelement is carried in a Wi-Fi Alliance Vendor Extension attribute with the Vendor Extension attribute ID set to 0x1049, Vendor ID set to 0x00372A, and the subelement ID set to 0x06. See Table 29 of [5].

If a BSS supports backhaul connections, a Multi-AP Controller shall include a Multi-AP Extension subelement in the AP-Autoconfiguration WSC containing an M2 with bit 6 of the subelement value set to one. If a Controller wants a backhaul BSS of a Multi-AP Agent that implements Profile-2 to disallow association to any Backhaul STA that would result in a Profile-1 backhaul link (as per section 12.1), a Multi-AP Controller shall include a Multi-AP Extension subelement in the AP-Autoconfiguration WSC containing an M2 with bit 6 of the subelement value set to one and bit 3 of the subelement value set to one. If a Controller wants a backhaul BSS of a Multi-AP Agent that implements Profile-2 to disallow association to any Backhaul STA that would result in a Profile-2 backhaul link (as per section 12.1), a Multi-AP Controller shall include a Multi-AP Extension subelement in the AP-Autoconfiguration WSC containing an M2 with bit 6 of the

subelement value set to one and bit 2 of the subelement value set to one. If a BSS supports fronthaul connections, a Multi-AP Controller shall include a Multi-AP Extension subelement in the AP-Autoconfiguration WSC containing an M2 with bit 5 of the subelement value set to one. The Wi-Fi Alliance Vendor Extension attribute shall be carried in ConfigData encrypted by the KeyWrapKey in the AP-Autoconfiguration WSC message containing an M2.

Table 7. Multi-AP Extension subelement

Field	Length	Value	Description
Subelement ID	1 octet	0x06	Multi-AP Extension subelement identifier.
Subelement Length	1 octet	0x01	Number of Bytes in the subelement value.
Subelement Value	bit 7	Variable	Backhaul STA
	bit 6	Variable	Backhaul BSS
	bit 5	Variable	Fronthaul BSS
	bit 4	Variable	Tear Down
	bit 3	Variable	Profile-1 Backhaul STA association disallowed.
	bit 2	Variable	Profile-2 Backhaul STA association disallowed.
	bits 1 - 0		Reserved

To facilitate one or more backhaul STAs acting as an enrollee to connect to a Multi-AP network, a Multi-AP Controller should indicate that at least one BSS on any of the Multi-AP Agent(s) is set to support Multi-AP backhaul connections.

If triggered¹, the Multi-AP Controller shall include a Multi-AP Extension subelement with bit 6 Backhaul BSS and/or bit 5 Fronthaul BSS set to one in the corresponding M2 in an AP-Autoconfiguration WSC message per section 17.1.3.

A Multi-AP Controller shall limit the number of WSC TLVs containing M2 in the AP-Autoconfiguration WSC message to no more than the value in the Maximum number of BSS(s) supported by this radio in the AP Radio Basic Capabilities TLV. A Multi-AP Controller shall set the Radio Unique Identifier field in the AP Radio Identifier TLV in the AP-Autoconfiguration WSC message to the value of the same field specified in the AP Radio Basic Capabilities TLV in the corresponding AP-Autoconfiguration WSC message received from the Multi-AP Agent.

If a Multi-AP Agent receives an AP-Autoconfiguration WSC message containing one or more M2, it shall validate each M2 (based on its 1905 AL MAC address) and configure a BSS on the corresponding radio for each of the M2. If the Multi-AP Agent is currently operating a BSS with operating parameters that do not completely match any of the M2 in the received AP-Autoconfiguration WSC message, it shall tear down that BSS. If a Multi-AP Agent receives an AP-Autoconfiguration WSC message containing an M2 with a Multi-AP Extension subelement with bit 4 (Tear Down bit) of the subelement value set to one (see Table 7), it shall tear down all currently operating BSS(s) on the radio indicated by the Radio Unique Identifier, and shall ignore the other attributes in the M2. If a Multi-AP Agent that implements Profile-2 receives an AP-Autoconfiguration WSC message for a backhaul BSS with bit 3 of the Multi-AP Extension subelement set to one, it shall configure such BSS to refuse association from backhaul STAs that would result in a Profile-1 backhaul, as per section 12. If a Multi-AP Agent that implements Profile-2 receives an AP-Autoconfiguration WSC message for a backhaul BSS with bit 2 of the Multi-AP Extension subelement set to one, it shall configure such BSS to refuse association from backhaul STAs that would result in a Profile-2 backhaul, as per section 12.

If a Multi-AP Agent that implements Profile-2 receives an AP-Autoconfiguration WSC with a Traffic Separation Policy TLV with the Number of SSIDs field set to a non-zero value and the Multi-AP Agent is unable to configure one or more BSS as indicated by the M2 TLVs and by the Traffic Separation Policy TLV, the Multi-AP Agent shall tear down each of those BSS and shall send an Error Response message per section 17.1.37 containing one Profile-2 Error Code TLVs with reason code field set to 0x07 or 0x08.

¹ This specification only partially defines the algorithms that govern the operation of a Multi-AP Controller. These Multi-AP Controller algorithms' actions are alluded to by the wording "If triggered, a Multi-AP Controller..." in this specification.

If a Multi-AP Agent receives an AP-Autoconfiguration Renew message, then it shall respond within one second by sending one AP-Autoconfiguration WSC message per section 17.1.3 for each of its radios, irrespective of the value specified in the SupportedFreqBand TLV in the AP-Autoconfiguration Renew message.

If a Multi-AP Agent that implements Profile-2 receives an AP-Autoconfiguration Renew message, then it shall retain all configuration and policy it has previously received in TLVs except those explicitly updated by the Autoconfig Renew procedure.

Note: A Multi-AP Agent that implements Profile-2 might check that the AP-Autoconfiguration Renew message is from the Multi-AP Controller with which it previously on-boarded (for example, by comparing the ALID of the Controller for the new request against the ALID of the original Controller) and ignore the message if not.

Table 8. Multi-AP Profile subelement

Field	Length	Value	Description
Subelement ID	1 octet	0x07	Multi-AP Profile subelement identifier.
Subelement Length	1 octet	0x01	Number of octets in the subelement value (subelement payload).
Subelement Value	1 octet	0x00: Reserved 0x01: Multi-AP Profile-1 0x02: Multi-AP Profile-2 0x03~0xFF: Reserved	Multi-AP Profile field.

7.2 AP operational BSS reporting

A Multi-AP Agent indicates the BSS(s) it is currently operating on each of its radios in the 1905 Topology Response message. A Multi-AP device treats each BSS as an IEEE 802.11 “local interface” specified in [2].

A Multi-AP Agent shall indicate each BSS that is operating in PWR_ON or PWR_SAVE mode as a separate (802.11) Local Interface in the Device Information Type TLV in the 1905 Topology Response message. The Multi-AP Agent shall set the MAC address of the Local Interface field in the Device Information Type TLV in the 1905 Topology Response message to the BSSID. A Multi-AP Agent shall include an AP Operational BSS TLV in the 1905 Topology Response message per section 17.1.4. The Multi-AP Agent shall indicate all BSS(s) it is currently operating in PWR_ON or PWR_SAVE mode on each of its radios in the AP Operational BSS TLV in the 1905 Topology Response message.

7.3 Policy configuration

The Multi-AP Policy Config Request message enables a Multi-AP Controller to configure Multi-AP control related policies on a Multi-AP Agent.

If triggered, a Multi-AP Controller shall send a Multi-AP Policy Config Request message per section 17.1.8 to a Multi-AP Agent. If a Multi-AP Agent receives a Multi-AP Policy Config Request message, then it shall respond within one second with a 1905 Ack message per section 17.1.32.

The Steering Policy TLV defined in section 17.2.11 contains steering related policies. The Local Steering Disallowed STA list indicates STAs that are only to be steered in response to a steering message indicating Steering Mandate from the Multi-AP Controller (see section 11.1). The BTM Steering Disallowed STA list indicates STAs that are to be steered using the Client Association Control mechanism (see section 11.6). The Steering Policy field indicates the policy for Multi-AP Agent-initiated steering on a given radio. The Channel Utilization Threshold and RCPI Steering Threshold fields indicate thresholds used in Agent-initiated steering for each radio.

The Metrics Reporting Policy TLV defined in section 17.2.12 contains link metrics reporting related policies. The AP Metrics Reporting Interval field indicates if periodic AP metrics reporting is to be enabled, and if so the cadence. The STA

Metrics Reporting RCPI Threshold and AP Metrics Channel Utilization Reporting Threshold fields indicate if threshold-based metric reporting is to be enabled for STA and/or AP metrics, and if so the corresponding thresholds for each radio.

The Channel Scan Reporting Policy TLV defined in section 17.2.37 identifies whether a Multi-AP Agent that implements Profile-2 is required to report the results of any Independent Channel Scan that it performs to the Multi-AP Controller.

The Unsuccessful Association Policy TLV defined in section 17.2.58 contains policies related to reporting unsuccessful associations. The Report Unsuccessful Associations bit indicates whether a Multi-AP Agent that implements Profile-2 shall report unsuccessful association attempts of client STAs. The Maximum Reporting Rate value indicates the maximum rate at which the unsuccessful associations shall be reported.

8 Channel selection

Multi-AP control messages enable the configuration of a Multi-AP Agent with parameters for channel selection.

8.1 Channel Preference Query and Report

Channel Preference Query and Channel Preference Report messages enable a Multi-AP Controller to query operating channel preferences for AP radios of a Multi-AP Agent.

If triggered, a Multi-AP Controller shall send a Channel Preference Query message per section 17.1.9 to a Multi-AP Agent.

If a Multi-AP Agent receives a Channel Preference Query message, then it shall respond within one second with a Channel Preference Report message per section 17.1.10. The Channel Preference Report message shall contain the same MID that was received in the Channel Preference Query message. The Channel Preference Report message shall contain information regarding all the channels that a given radio of the Multi-AP Agent transmitting the report is temporarily unable to operate in, or prefers not to operate in, for each supported operating class as specified by the Multi-AP Agent (per Operating Classes field in the AP Radio Basic Capabilities TLV in section 17.2.7). Additionally, the Channel Preference Report message shall contain information regarding the channel separation (if any) that a given radio of the Multi-AP Agent requires between each of its own potential operating channels and the operating channel of another radio of the Multi-AP Agent, where the two radios may have one transmitting and the other receiving or transmitting simultaneously.

Note: Channels for which the Multi-AP Agent's radio is statically (permanently) unable to operate are reported in the AP Radio Basic Capabilities TLV. A Channel Preference Report message does not include information on operating classes that are not supported by the corresponding radio of the Multi-AP Agent per the AP Radio Basic Capabilities TLV.

If a Multi-AP Controller receives a Channel Preference Report message from a Multi-AP Agent, the Multi-AP Controller shall delete all (if any) previously stored channel preference information from the Multi-AP Agent pertaining to all radios of that Multi-AP Agent and replace it with the information contained within the Channel Preference Report message.

If a Channel Preference Report does not specify a preference for a particular channel within a supported operating class as specified by the Multi-AP Agent for a given radio, the Multi-AP Controller shall infer that the Multi-AP Agent is indicating the highest preference (preference score 15) for the channel in that operating class on the corresponding radio. If a Channel Preference Report contains zero Channel Preference TLVs and zero Radio Operation Restriction TLVs, the Multi-AP Controller shall infer that the Multi-AP Agent is indicating the highest preference (preference score 15) for all channels and operating classes supported by all of the Multi-AP Agent's radios.

The mechanism by which a Multi-AP Agent determines and reevaluates its channel preferences is implementation-specific. However, a Multi-AP Agent shall indicate a channel is operable when indicating preferences in a Channel Preference Report with the following exceptions:

- If a radio cannot operate on a channel in an operating class due to detection of radar, that channel shall be indicated as a Non-operable channel
- If conditions exist whereby normal operation of a BSS by the radio on a channel would be unsuccessful (e.g. due to strong interference), the channel shall be indicated as a Non-operable channel.

If a Multi-AP Agent's channel preferences change, it shall send an unsolicited Channel Preference Report to the Multi-AP Controller indicating the Multi-AP Agent's current preferences.

If a Multi-AP Agent detects a change in the DFS status of any channel, it shall send an unsolicited Channel Preference Report to the Controller setting the appropriate DFS related Reason Code for the channel per Table 23 of section 17.2.13.

If a Multi-AP Controller receives an unsolicited Channel Preference Report message, then it shall respond within one second with a 1905 Ack message.

8.2 Channel Selection Request and Report

The Channel Selection Request message contains information regarding the Multi-AP Controller's preferences and restrictions for the operating classes, channels and transmit power for each radio of a Multi-AP Agent.

If triggered, a Multi-AP Controller shall send a Channel Selection Request message per section 17.1.11.

If a Multi-AP Controller sends a Channel Selection Request message, it shall specify an “operable” preference for at least one of the non-DFS channels that the Multi-AP Agent indicated as operable (i.e. that the Multi-AP Agent did not explicitly indicate the channel as a Non-operable channel) on each radio of the Multi-AP Agent per the most recently received Channel Preference Report message and AP Radio Basic Capabilities TLV from the Multi-AP Agent.

If a Multi-AP Controller sends a Channel Selection Request message, it shall not specify preferences in which the only allowed channels for a given radio violate the radio operation restrictions indicated in the most recently received Channel Preference Report message from the Multi-AP Agent.

If a Multi-AP Controller sends a Channel Selection Request message, it should specify preferences that take into account the corresponding preference values indicated by the Multi-AP Agent in the most recent Channel Preference Report message. Except where necessary for load balancing or other network management requirements, the Multi-AP Controller should refrain from indicating a preference of Non-operable channel for a channel and operating class that the Multi-AP Agent has indicated is operable on a given radio.

If a Multi-AP Agent receives a Channel Selection Request message from the Multi-AP Controller, the Multi-AP Agent shall delete all (if any) previously stored channel preference information from the Multi-AP Controller pertaining to all radios of the Multi-AP Agent and replace it with the information contained within the message. A Multi-AP Agent shall store the channel preference information in non-volatile storage. If a Multi-AP Agent reboots, it may either continue to use the most recent channel preference information received from the Multi-AP Controller prior to the reboot, or it may flush any previously received channel preference information and assume all supported channels are preferred until such time that new channel preference information is received from the Multi-AP Controller.

If a Channel Selection Request message does not specify a preference for a particular channel within a supported operating class as specified by the Multi-AP Agent for a given radio, the Multi-AP Agent shall infer that the Multi-AP Controller is indicating the highest preference (preference score 15) for the channel in that operating class on the corresponding radio. If a Channel Selection Request message contains zero Channel Preference TLVs, the Multi-AP Agent shall infer that the Multi-AP Controller is indicating the highest preference (preference score 15) for all channels and operating classes supported by all of the Multi-AP Agent's radios.

A Multi-AP Agent shall not operate a radio on a channel and operating class for which the currently stored Multi-AP Controller preference information indicates as a Non-operable channel.

If a Multi-AP Agent receives a Channel Selection Request message from the Multi-AP Controller, it shall attempt to operate each of its radios on one of the channels indicated as the highest preference for that radio per the Channel Selection Request message.

If a Multi-AP Agent attempts to operate, or is already operating, a radio on a channel and that channel becomes an Inoperable channel, the Multi-AP Agent should take into account the corresponding preference values indicated in the most recently received Channel Selection Request message (if any). The exact mechanism by which the Multi-AP Agent selects the operating channel(s) and operating class(es) is implementation-specific.

If a Multi-AP Agent performs Channel availability check (CAC), it should take into account the channel prioritization in the Channel Selection Request message when deciding which channels to check first.

A Multi-AP Agent should operate a radio at the maximum nominal transmit power the radio is capable of operating and is allowed to operate according to applicable regulatory rules. If a Multi-AP Agent receives a Channel Selection Request message containing a Transmit Power Limit TLV, it shall limit the nominal transmit power of the corresponding radio to the value specified in the TLV.

If a Multi-AP Agent receives a Channel Selection Request message, it shall within one second send a Channel Selection Response message (section 17.1.12) to the Multi-AP Controller indicating, for each radio, whether the Multi-AP Agent accepts or declines the request and, if appropriate, the reason for declining. The Channel Selection Response message shall contain the same MID that was received in the Channel Selection Request message.

If a Multi-AP Agent sent a Channel Selection Response message indicating acceptance of the Multi-AP Controller's request for a given radio, the Multi-AP Agent shall make any necessary adjustments to the operating channel, operating classes and transmit power of its radios and then, irrespective of whether any adjustments have been made, send an Operating Channel Report message per section 17.1.13 containing information regarding the current operating parameters for each of the Multi-AP Agent's radios.

If a Multi-AP Controller receives an Operating Channel Report message, then it shall respond within one second with a 1905 Ack message.

If a Multi-AP Agent changes the operating channel, operating class and/or nominal transmit power of a radio of its own accord (i.e. not in response to reception of a Channel Selection Request message), then it shall send an unsolicited Operating Channel Report message per section 17.1.13 to the Multi-AP Controller indicating the new operating parameters for the corresponding radio.

Note: The operating classes specified in an Operating Channel Report TLV are equal to the values indicated in the Operating Classes field of the Supported Operating Classes element (per section 9.4.2.54 of [1]), if the Supported Operating Classes element is transmitted by the AP operating in the BSS on the corresponding radio. This includes an operating class corresponding to each channel bandwidth in which the radio is currently operating (e.g. typically 20, 40 and 80 MHz Operating Classes for a VHT80 AP). When a primary channel is used, the 20 MHz Operating Class indicates that primary channel.

8.2.1 Coordinated DFS CAC

A Multi-AP network provides the ability for a Multi-AP Controller to request that Multi-AP Agents perform Channel Availability Checks (CACs), or provide their CAC status. The Multi-AP Agents report the result of the requested CACs and report their CAC status if requested. These features provide assistance in efficiently meeting the regulatory requirements in various geographies.

8.2.2 DFS CAC Scan Requirements on a Multi-AP Controller

If triggered, a Multi-AP Controller shall send a CAC Request message to a Multi-AP Agent, requesting one or more CACs. The Multi-AP Controller should not send another CAC request to a given Radio Unique Identifier until the previous CAC request has completed or has been terminated.

A Multi-AP Controller shall not send a CAC Request TLV of a method, operating class, or on an operating channel outside the Multi-AP Agent's most recently received CAC Capabilities TLV (see section 17.2.46).

If triggered, a Multi-AP Controller shall send a CAC Termination message to a Multi-AP Agent.

If a Multi-AP Controller receives a Channel Preference Report message (see section 8.1) with a CAC Status Report TLV, it may consider spectrum available in one channel/class pair to be available in all channel/class pairs that include that spectrum.

If triggered, a Multi-AP Controller may send a Channel Selection Request with a Controller DFS Channel Clear Indication.

8.2.3 DFS CAC Scan Requirements on a Multi-AP Agent

If a Multi-AP Agent receives a CAC Request message from a Multi-AP Controller, it shall respond within one second with a 1905.1 Ack.

If a Multi-AP Agent receives a CAC Request message from a Multi-AP Controller, it may decline to perform the CAC by sending a Channel Preference Report message (see section 8.1) with a CAC Completion Report TLV with the CAC Completion Status field indicating a CAC failure.

If a Multi-AP Agent receives a CAC Request message from a Multi-AP Controller, and does not decline the request, then it shall commence a CAC on the requested channel, using the requested CAC type and bandwidth, within 15 seconds.

If a Multi-AP Agent receives a CAC Request message that contains more than one CAC request, and it is unable to perform them simultaneously, it may perform them sequentially, in any order it chooses.

If a Multi-AP Agent is performing a CAC and a Multi-AP Agent receives a CAC request for a different CAC method, bandwidth, or channel, on a given radio unique identifier, then it shall terminate any current CAC and begin a new CAC according to the new request within 15 seconds. If a Multi-AP Agent terminates an ongoing CAC due to receiving a new CAC Request, the Multi-AP Agent shall not send a Channel Preference Report message for the terminated CAC.

If a Multi-AP Agent is performing a CAC and receives a CAC Termination message, it shall respond within one second with a 1905.1 ACK, terminate any ongoing CAC, and return the radio that was performing the CAC to its most recent operational configuration. The Multi-AP Agent shall not send a Channel Preference Report message for the terminated CAC.

If a Multi-AP Agent performing a CAC encounters any of the following three conditions:

- The full time required for the CAC has elapsed
- An error occurs which prevents continuing the CAC
- Radar is detected

then within 15 seconds a Multi-AP Agent shall send an unsolicited Channel Preference Report, and include a CAC Completion Report TLV and a Channel Preference TLV for the radio that experienced one of the three conditions. If a Multi-AP Agent sends a Channel Preference Report with a CAC Completion Report TLV that indicates detection of radar has occurred, the Multi-AP Agent may indicate which sub-channel(s) the radar appeared in.

If a Multi-AP Agent sends a CAC Channel Preference report with a CAC Completion Report TLV that indicates which sub-channel(s) the radar appeared in, the report may include indications only at the lowest bandwidth classes to which the radar could be isolated.

Upon completion of a requested CAC, if a CAC was a Successful CAC, the Multi-AP Agent shall follow the CAC Completion Action specified in the CAC Request. If a CAC was an Unsuccessful CAC, the Multi-AP Agent shall return the radio that was performing the CAC to its most recent operational configuration.

If a Multi-AP Agent sends an unsolicited Channel Preference Report with a Reason Code "0111", this Channel Preference Report shall be sent within 15 seconds of detecting the radar or within 15 seconds of being re-connected to the network after detecting the radar.

If a Multi-AP Agent sends a Channel Preference Report message for any reason, the Multi-AP Agent shall include Channel Preference TLVs for all radios in the Multi-AP Agent, and a CAC Status Report TLV. The Channel Preference TLVs and CAC Status Report TLV shall include a list of the Available Channels. The Channel Preference TLVs and CAC Status Report TLV shall also include a list of the non-occupancy channels and the Non-Occupancy Duration remaining on those channels. The Multi-AP Agent should report Non-Occupancy Channels in the lowest bandwidth class to which the radar could be isolated.

The CAC status report shall include the status of any ongoing CAC for all radios within the Multi-AP Agent.

If a Multi-AP Agent receives a Channel Selection Request with a Controller DFS Channel Clear Indication, it may change to that channel without performing a CAC on that channel.

9 Capability information reporting

9.1 AP capability

AP Capability Query and AP Capability Report messages enable a Multi-AP Controller or a Multi-AP Agent to obtain the capability information of all AP radios on a Multi-AP device.

If triggered, a Multi-AP Controller or a Multi-AP Agent shall send an AP Capability Query message per section 17.1.6. If a Multi-AP Agent receives an AP Capability Query message, then it shall respond within one second with an AP Capability Report message per section 17.1.7. A Multi-AP Agent shall include one AP Capability TLV in the AP Capability Report message. A Multi-AP Agent shall include one AP Radio Basic Capabilities TLV for each AP radio in the AP Capability Report message. A Multi-AP Agent that implements Profile-2 shall include one Metric Collection Interval TLV in the AP Capability Report message.

If an AP radio supports 802.11 High Throughput capability, a Multi-AP Agent shall include an AP HT Capabilities TLV for that radio in the AP Capability Report message. If an AP radio supports 802.11 Very High Throughput capability, a Multi-AP Agent shall include an AP VHT Capabilities TLV for that radio in the AP Capability Report message. If an AP radio supports 802.11 High Efficiency capability, a Multi-AP Agent shall include an AP HE Capabilities TLV for that radio in the AP Capability Report message.

If an AP radio managed by a Multi-AP Agent is capable of multiple virtual radio operation (see Table 1), then the Multi-AP Agent shall identify each of the virtual radios separately with a unique Radio unique identifier in the capabilities TLVs and indicate capability information only pertaining to indicated virtual radio in the capabilities TLVs in the AP Capability Report message.

If a Multi-AP Agent that implements Profile-2 sends an AP Capability Report message, it shall perform the following:

- Include one Channel Scan Capabilities TLV in the AP Capability Report message. Operating classes specified in this TLV shall be 20 MHz operating classes from Table E-4 of [1]. If the "On boot only" bit is set to one, the Scan Impact field shall be set to 0x00.
- Include one CAC Capabilities TLV in an AP Capabilities Report message. A Multi-AP Agent may restrict its reported CAC capabilities to match the regulations of the country in which it is operating. The CAC Capabilities TLV shall include an indication of the country in which the Multi-AP Agent is operating according to the two letter codes provided in [6]. The Multi-AP Agent shall specify CAC capabilities for each Simultaneous CAC Radio in the Multi-AP Agent.
- Include one Profile-2 AP Capability TLV in the AP Capability Report message.

If a Multi-AP Agent that implements Profile-2 sends a Profile-2 AP Capability TLV, it shall perform the following:

- Set the Byte Counter Units field to 0x01 (KiB (kibibytes)).
- Set the Max Total Number of VIDs field to 2 or greater.
- If the Multi-AP Agent onboards to a Multi-AP Controller that implements Profile-1, the Multi-AP Agent shall set the Byte Counter Units field to 0x00 (bytes) and report the values of the BytesSent and BytesReceived fields in the Associated STA Traffic Stats TLV in bytes.

The AP Capability Report message shall contain the same MID that was received in the AP Capability Query message.

9.2 Client capability

Multi-AP Client Capability Query and Client Capability Report messages enable a Multi-AP Controller to obtain capability information of a client STA associated with a Multi-AP Agent.

If triggered, a Multi-AP Controller shall send a Client Capability Query message per section 17.1.14. If triggered and supported, a Multi-AP Agent shall send a Client Capability Query message per section 17.1.14.

If a Multi-AP Agent receives a Client Capability Query message, then within one second it shall respond with a Client Capability Report message per section 17.1.15. The Client Capability Report message shall contain the same MID that was received in the Client Capability Query message. If the STA specified in the Client Capability Query message is not associated with any of the BSS operated by the Multi-AP Agent (an error scenario), the Multi-AP Agent shall set the result code in the Client Capability Report TLV to 0x01 per section 17.2.19 and include an Error Code TLV with the reason code

set to 0x02 and the STA MAC address field included per section 17.2.36 in the Client Capability Report message. If the STA specified in the Client Capability Query message is associated with any of the BSS operated by the Multi-AP Agent and the Multi-Agent is unable to report the client's capability, the Multi-AP Agent shall set the result code in the Client Capability Report TLV to 0x01 and include an Error Code TLV with the reason code set to 0x03 in the Client Capability Report message.

9.3 Backhaul STA capability

Backhaul STA Capability Query and Backhaul STA Capability Report messages enable a Multi-AP Controller to obtain the capability information of all backhaul STA radios on a Multi-AP device.

If triggered, a Multi-AP Controller shall send a Backhaul STA Capability Query message per section 17.1.42. If a Multi-AP Agent receives a Backhaul STA Capability Query message, then it shall respond within one second with a Backhaul STA Capability Report message per section 17.1.43. A Multi-AP Agent shall include one Backhaul STA Radio Capabilities TLV for each Backhaul STA radio in the Backhaul STA Capability Report message.

The Backhaul STA Capability Report message shall contain a MID that was indicated in a previously received Backhaul STA Capability Query message.

10 Link metric collection

10.1 Backhaul link metrics

This section defines the protocol for a Multi-AP device to convey backhaul link metric information associated with each of the BSSs in which the Multi-AP device is operating.

The 1905 link metric information dissemination protocol is used to query and report link metrics for backhaul links (e.g. link between a Multi-AP Agent AP interface and a Multi-AP Agent backhaul STA interface, or between two Multi-AP Agent Ethernet interfaces. See [2]).

If triggered, a Multi-AP Controller and Multi-AP Agent shall send a 1905 Link metric query message to a Multi-AP Agent.

Note: Additional clarifications with respect to fields in a 1905 Transmitter link metric TLV are as follows:

- **macThroughputCapacity** field is the estimated MAC data rate in Mb/s for the backhaul link in the downlink direction when reported by a Multi-AP Agent that operates the AP for the link, or the estimated MAC data rate in Mb/s for the backhaul link in the uplink direction when reported by the Multi-AP Agent that operates the backhaul STA for the link, if 100% of channel air time and BSS operating bandwidth were to be available.
- **linkAvailability** field is the predicted percentage of Air Time that the backhaul link would consume given the current channel condition, assuming sufficient BE traffic is generated over the backhaul link to the client STAs and/or other backhaul STAs associated with the downstream Multi-AP Agent to fill this Air Time.

Note: Additional clarifications with respect to fields in a 1905 Receiver link metric TLV are as follows:

- The **RSSI** field is calculated from the RCPI of a number of PPDU received when reported by a Multi-AP Agent that operates the AP for the link, or the Beacon RSSI when reported by a Multi-AP Agent that operates the backhaul STA for the link.

Note: A Multi-AP Agent supporting [11] might use the transmitter and receiver Link metric TLVs as defined in [11] to report the metrics of Generic Phy non-Wi-Fi interfaces.

10.2 Per-AP metrics and bulk STA metrics

This section defines the protocol for a Multi-AP Agent to convey per-AP metric information about each of the BSS (fronthaul and/or backhaul) it is operating. These metrics pertain to the BSS overall, and can also include information relating to every STA associated to the AP. For metrics relating to a single specific STA that might be associated to the BSS, see section 10.3.

10.2.1 Link metric measurements from the AP

If triggered, a Multi-AP Controller shall send an AP Metrics Query message per section 17.1.16 to a Multi-AP Agent.

If a Multi-AP Agent receives an AP Metrics Query message, then it shall respond within one second with an AP Metrics Response message (section 17.1.17) containing the following TLVs:

- One AP Metrics TLV per section 17.2.22 for each of the BSSs specified in the query.
- If the Multi-AP Agent implements Profile-2, it shall include one AP Extended Metrics TLV for each of the BSSs specified in the query.
- If the Multi-AP Agent implements Profile-2, it shall include one Radio Metrics TLV for each of the radios specified in the query.

The AP Metrics Response message shall contain the same MID that was received in the AP Metrics Query message.

If a Multi-AP Agent receives a Metric Reporting Policy TLV with AP Metrics Reporting Interval field set to a non-zero value, it shall send an AP Metrics Response message to the Multi-AP Controller once every reporting interval specified in the field and containing the following TLVs:

- One AP Metrics TLV for each BSS which it is operating.

- If the Multi-AP Agent implements Profile-2, it shall include one AP Extended Metrics TLV for each BSS which it is operating
- If the Multi-AP Agent implements Profile-2, it shall include one Radio Metrics TLV for each radio which it is operating.

If a Multi-AP Agent receives a Metric Reporting Policy TLV with AP Metrics Channel Utilization Reporting Threshold field set to a non-zero value for a given radio, it shall measure the channel utilization on that radio in each consecutive implementation-specific measurement period and, if the most recently measured channel utilization has crossed the reporting threshold in either direction (with respect to the previous measurement), it shall send an AP Metrics Response message to the Multi-AP Controller containing the following TLVs:

- One AP Metrics TLV for each of the BSSs on that radio.
- If the Multi-AP Agent implements Profile-2, it shall include one AP Extended Metrics TLV for each of the BSSs on that radio.
- If the Multi-AP Agent implements Profile-2, it shall include one Radio Metrics TLV for that radio.

If a Multi-AP Agent sends an AP Extended Metrics TLV, it shall encode the byte counters in that TLV according to the value of the Byte Counter Units field in its last sent Profile-2 AP Capability TLV (if the Multi-AP Agent implements Profile-2), or in bytes if it has not sent a Profile-2 AP Capability TLV.

If a Multi-AP Agent sends an AP Metrics Response message and if the most recently received (if any) Metric Reporting Policy TLV has Associated STA Traffic Stats Inclusion Policy set to one for a specified radio, the Multi-AP Agent shall also include one Associated STA Traffic Stats TLV for each STA associated to a BSS being reported on that radio unless it has sent a previous AP Metrics Response message including the corresponding STA Traffic Stats TLVs within the previous 10 seconds, in which case it may include or omit the STA Traffic Stats TLVs.

If a Multi-AP Agent sends an Associated STA Traffic Stats TLV, it shall encode the byte counters in that TLV according to the value of the Byte Counter Units field in its last sent Profile-2 AP Capability TLV (if the Multi-AP Agent implements Profile-2), or in bytes if it has not sent a Profile-2 AP Capability TLV.

If a Multi-AP Agent sends an AP Metrics Response message and if the most recently received (if any) Metric Reporting Policy TLV has Associated STA Link Metrics Inclusion Policy set to one for a specified radio, the Multi-AP Agent shall also include one Associated STA Link Metrics TLV and if the Multi-AP Agent implements Profile-2 one Associated STA Extended Link Metrics TLV for each STA associated to a BSS being reported on that radio.

When reporting STA Traffic Stats, a Multi-AP Agent should report the most recent counter information commensurate with maintaining AP throughput performance, and shall report counter information no older than 10 seconds.

Note: The Estimated Air Time Fraction subfield in the Estimated Service Parameters Information field in an AP Metrics TLV is defined in 9.4.2.174 of [1] and represents the predicted percentage of air time that a new STA joining the BSS would be allocated for data PPDUs (transmitted downlink from the AP) carrying data of the corresponding AC for the STA. For the purpose of defining the Estimated Air Time Fraction value, it is assumed that the downlink traffic load to the hypothetical newly joining STA is sufficient to fill the estimated air time fraction.

10.2.2 Channel Scan

A Multi-AP network managed by a Multi-AP Controller that implements Profile-2 provides the ability for Multi-AP Agents to perform a set of channel scans and report the results of the scans to the Multi-AP Controller. A Multi-AP Agent has the capability to perform a set of channel scans either at boot only, or upon request from the Multi-AP Controller.

10.2.2.1 Channel Scan Requirements on a Multi-AP Controller

If triggered, a Multi-AP Controller shall send a Channel Scan Request message (see section 17.1.33) to a Multi-AP Agent.

If a Multi-AP Controller sends a Channel Scan Request to a Multi-AP Agent with the Perform Fresh Scan bit set to zero, it shall set the Number of Operating Classes field for each radio listed to zero.

A Multi-AP Controller shall not send a Channel Scan Request to a Multi-AP Agent that implements Profile-1.

If a Multi-AP Controller receives a Channel Scan Report message, it shall respond within one second with a 1905 Ack message.

10.2.2.2 Channel Scan Requirements on a Multi-AP Agent

If a Multi-AP Agent receives a Channel Scan Request message, it shall respond within one second with a 1905 Ack message.

On-Boot Scan

If a Multi-AP Agent sets the "On boot only" bit to 1 in its Channel Scan Capabilities TLV, it shall perform a Channel Scan at boot on each of the radio and operating class and channel combinations specified in its Channel Scan Capabilities and shall store the scan results.

Requested Channel Scan - Fresh

If a Multi-AP Agent has set the "On boot only" bit to 0 in its Channel Scan Capabilities TLV and receives from the Multi-AP Controller a Channel Scan Request message containing a Channel Scan Request TLV with the "Perform Fresh Scan" bit set to one and the Multi-AP Agent is currently performing a Requested Channel Scan, the Multi-AP Agent should abort the current Requested Channel Scan as soon as practical and shall send to the Multi-AP Controller a Channel Scan Report Message relating to that Channel Scan before acting on the new request as described in the following paragraph.

If a Multi-AP Agent that has set the "On boot only" bit to 0 in its Channel Scan Capabilities TLV receives from the Multi-AP Controller a Channel Scan Request message containing a Channel Scan Request TLV with the "Perform Fresh Scan" bit set to one and is not currently performing a Requested Channel Scan, the Multi-AP Agent shall, as soon as practical, start a sequence of Channel Scans on the requested radio and operating class and channel combinations. When finished scanning, or within 5 minutes, whichever comes sooner, the Multi-AP Agent shall send to the Multi-AP Controller a Channel Scan Report Message (see section 17.1.34) containing one Timestamp TLV (see section 17.2.41) indicating the current time and one Channel Scan Result TLV (see 17.2.40) for each of the operating class and channel combinations listed in the Channel Scan Request TLV. Each Channel Scan Result TLV shall contain either a success Status Code and the scan result data or a non-Success Scan Status code, as defined in Table 50, indicating the reason the scan could not be completed. The Multi-AP Agent shall set the Status Code as follows:

If the requested Channel Scan operating class and channel combination is in the set of operating class and channel combinations in the Multi-AP Agent's declared Channel Scan Capabilities and the Multi-AP Agent successfully completed the fresh Channel Scan, the Multi-AP Agent shall set the Status Code to 0x00 (Success).

If the requested Channel Scan operating class and channel combination is not in the set of operating class and channel combinations in the Multi-AP Agent's declared Channel Scan Capabilities, the Multi-AP Agent shall set the Status Code to 0x01.

If the Multi-AP Agent received the Channel Scan Request less than the Minimum Scan Interval declared in the Multi-AP Agent's Channel Scan Capabilities after the previously received Channel Scan Request, the Multi-AP Agent may set the Status Code to 0x02 and not perform the Channel Scan.

If the Multi-AP Agent has not performed the Channel Scan because the radio is too busy, the Multi-AP Agent shall set the Status Code to 0x03.

If the Multi-AP Agent has not been able to complete the Channel Scan in the time available, the Multi-AP Agent shall set the Status Code to 0x04.

If the Multi-AP Agent has aborted the Channel Scan due to receiving another Channel Scan Request, the Multi-AP Agent shall set the Status Code to 0x05.

The Multi-AP Agent shall store the result of the last successful scan on each radio and operating class and channel combination.

If a Multi-AP Agent has set the "On boot only" bit to 1 in its Channel Scan Capabilities TLV and receives from the Multi-AP Controller a Channel Scan Request message containing a Channel Scan Request TLV with the "Perform Fresh Scan" bit set to one, the Multi-AP Agent shall respond with a Channel Scan Report Message containing one Timestamp TLV indicating the current time and one Channel Scan Result TLV for each of the operating class and channel combinations listed in the Channel Scan Request TLV and set the Status Code to 0x06.

Requested Channel Scan - Stored

If a Multi-AP Agent receives a Channel Scan Request message containing a Channel Scan Request TLV with the "Perform Fresh Scan" bit set to zero, the Multi-AP Agent shall respond with a Channel Scan Report Message (see 17.1.34) containing one Timestamp TLV (see section 17.2.41) indicating the current time and one Channel Scan Result TLV (see 17.2.40) for each of the operating class and channel combinations for which it has stored results for each of the radios listed in the Channel Scan Request TLV, even if the Channel Scan Result is from an Independent Channel Scan and the "Report Independent Channel Scans" flag was set to zero in the most recently received Channel Scan Reporting Policy TLV. If the Multi-AP Agent has set the "On boot only" bit to 1 in its Channel Scan Capabilities TLV and has not yet completed the On-boot Scan on an operating class and channel combination listed in its Channel Scan Capabilities TLV, the Multi-AP Agent shall also include a Channel Scan Result TLV for that operating class and channel combination with the Status Code set to 0x04.

Independent Channel Scan

A Multi-AP Agent may perform an Independent Channel Scan.

If a Multi-AP Agent performs a set of Independent Channel Scans, and the "Report Independent Channel Scans" flag was set to one in the most recently received Channel Scan Reporting Policy TLV, then the Multi-AP Agent shall report the channel scan results to the Multi-AP Controller in a Channel Scan Report message as described above in Section 10.2.2.2 for a fresh Requested Channel Scan.

If a Multi-AP Agent performs a set of Independent Channel Scans, and has not received a Channel Scan Reporting Policy TLV, then the Multi-AP Agent shall not report the channel scan results to the Multi-AP Controller.

If the number of neighbors detected during a channel scan would mean that the channel scan report message would not fit within one 1905.1 CMDU, the Multi-AP Agent shall split the channel scan report across multiple Channel Scan Result TLVs by splitting the information related to sets of neighbor BSSs into separate Channel Scan Result TLVs and setting the NumberOfNeighbors field to the number of neighbors contained in the corresponding TLV.

10.3 Per-STA measurements

This section defines the protocol for a Multi-AP Agent to convey link metric information on a per-STA basis.

10.3.1 Associated STA link measurements from the AP

This subsection defines the protocol for a Multi-AP Agent to report link quality metrics for the downlink and uplink links between a Multi-AP Agent AP and an associated STA.

If triggered, a Multi-AP Controller shall send an Associated STA Link Metrics Query message per section 17.1.18 to a Multi-AP Agent.

If a Multi-AP Agent receives an Associated STA Link Metrics Query message, then it shall respond within one second with an Associated STA Link Metrics Response message per section 17.1.19 containing one Associated STA Link Metrics TLV and if the Multi-AP Agent implements Profile-2 one Associated STA Extended Link Metrics TLV for the specified STA. The Associated STA Link Metrics Response message shall contain the same MID that was received in the Associated STA Link Metrics Query message. If the specified STA is not associated with any of the BSS operated by the Multi-AP Agent (an error scenario), the Multi-AP shall set the Number of BSSIDs reported field in the Associated STA Link Metrics TLV to zero per section 17.2.24 and include an Error Code TLV with the reason code field set to 0x02 and the STA MAC address field included per section 17.2.36.

If a Multi-AP Agent receives a Metric Reporting Policy TLV with STA Metrics Reporting RCPI Threshold field set to a non-zero value for a given radio, the Multi-AP Agent shall monitor the uplink RCPI for each STA associated to a BSS operating on that radio and, if the most recently measured uplink RCPI for a STA has crossed the STA Metrics Reporting RCPI Threshold including hysteresis margin in either direction (with respect to the previous measurement), the Multi-AP Agent shall send an Associated STA Link Metrics Response message to the Multi-AP Controller containing an Associated STA Link Metrics TLV and if the Multi-AP Agent implements Profile-2 one Associated STA Extended Link Metrics TLV corresponding to that STA. Unless STA Metrics Reporting RCPI Hysteresis Margin Override field is set to a non-zero value in the most recently received Metric Reporting Policy TLV (if any) relating to a given radio, a Multi-AP Agent should use a non-zero implementation-specific hysteresis margin that is sufficient to avoid excessive generation of Associated

STA Link Metrics Response messages caused by rapid fluctuations of uplink RCPI measurements around the RCPI threshold and the Multi-AP Agent shall not use a hysteresis margin that is greater than 5 dB. If STA Metrics Reporting RCPI Hysteresis Margin Override field is set to a non-zero value in the most recently received Metric Reporting Policy TLV, a Multi-AP Agent shall use the value specified for STA Metrics Reporting RCPI Hysteresis Margin Override field as RCPI hysteresis margin when determining when to send an Associated STA Link Metrics Response message for RCPI threshold based reporting.

When a Multi-AP Agent measures RCPI or SNR values for the purpose of calculating the Estimated MAC Data Rate and uplink RCPI used for STA metric reporting, these values may be averaged over time using an implementation-specific smoothing function. When a non-zero STA Metrics Reporting RCPI Threshold is configured, a Multi-AP Agent should perform sufficient smoothing of uplink RCPI measurements to avoid excessive generation of Associated STA Link Metrics Response messages caused by measurement noise.

If a Multi-AP Agent sends an Associated STA Link Metrics TLV, it shall set the values of the Estimated MAC Data Rate metrics for downlink and uplink of the associated link based on the most recently measured uplink and downlink RCPI or SNR values. The Estimated MAC Data Rate metric is an estimate of the MAC layer throughput achievable on the link if 100% of channel air time and BSS operating bandwidth were to be available. The algorithm used by the Multi-AP Agent to calculate the Estimated MAC Data Rate metrics is implementation-specific. A reference method² is defined in Annex R.7 of [1], which takes RCPI or SNR as inputs, and where with respect to Equation R-1,

$$\text{Estimated MAC Data Rate} = \frac{MPDU_{pPPDU} \times A_{MSDU_B} \times 8}{PPDU_{Dur}}$$

10.3.2 Unassociated STA RCPI measurements from the AP

This subsection defines the protocol for a Multi-AP Agent to report uplink RCPI for unassociated STAs.

If triggered, a Multi-AP Controller and Multi-AP Agent shall send an Unassociated STA Link Metrics Query message per section 17.1.20 to a Multi-AP Agent.

A Multi-AP Controller and Multi-AP Agent shall not send an Unassociated STA Link Metrics Query message to a Multi-AP Agent that does not indicate support for Unassociated STA Link Metrics in the AP Capability TLV.

If a Multi-AP Agent that indicates support for Unassociated STA Link Metrics receives an Unassociated STA Link Metrics Query message, it shall respond within one second with a 1905 Ack message and attempt to measure the uplink RCPI for the specified STAs. If any of the STAs specified in the Unassociated STA Link Metrics Query message is associated with any BSS operated by the Multi-AP Agent (an error scenario), for each of those associated STAs, the Multi-AP Agent shall include an Error Code TLV with the reason code field set to 0x01 and the STA MAC address field included per section 17.2.36 in the 1905 Ack message. A Multi-AP Agent shall attempt RCPI measurement on the current operating channel(s) of its radio(s) and, if it indicated support with the Off-Channel Unassociated STA Link Metrics bit in the AP Capability TLV, shall attempt RCPI measurement on the other channels and Operating Classes specified in the query. When a Multi-AP Agent measures RCPI values for unassociated STA link metric reporting, these values may be averaged over time using an implementation-specific smoothing function.

If the Multi-AP Agent has collected one or more uplink RCPI measurements, it shall send an Unassociated STA Link Metrics Response message per section 17.1.21. A Multi-AP Agent may send the uplink RCPI measurements in one or more Unassociated STA Link Metrics Response messages immediately after some of the measurements become available or may bundle into a single Unassociated STA Link Metrics Response message. If the Multi-AP Agent cannot obtain any RCPI measurements on all of the STAs specified in the Unassociated STA Link Metrics Query message after some implementation-specific timeout, the Multi-AP Agent shall set the number of STAs included field in the Unassociated STA Link Metrics Response message to zero per section 17.2.26.

If a Multi-AP Controller receives an Unassociated STA Link Metrics Response message, then it shall respond within one second with a 1905 Ack message.

² In Equation R-2, P_{adjust} should take into account the expected interference caused by OBSS and other external interferers, as well as the expected inter-stream MU-MIMO interference (if applicable). "Inbound" indicates uplink direction, while "Outbound" indicates downlink direction

10.3.3 802.11 beacon measurements from the client

This subsection defines the protocol to request a Multi-AP Agent to obtain 802.11 Beacon Report measurements from an associated STA and respond with the Beacon Report from that STA. The primary purpose is to obtain measurements of downlink RCPI from Beacon or Probe Response frames transmitted by the AP operating in a BSS, as the basis for steering decisions, however the mechanism can also be used to obtain Information Elements from the Beacon or Probe Response frames transmitted by the APs operating in those BSSs.

If triggered, a Multi-AP Controller and Multi-AP Agent shall send a Beacon Metrics Query message per section 17.1.22 to a Multi-AP Agent.

If a Multi-AP Agent receives a Beacon Metrics Query message, then it shall respond within one second with a 1905 Ack message. If the specified STA in the Beacon Metrics Query message is not associated with any of the BSS operated by the Multi-AP Agent (an error scenario), the Multi-AP Agent shall include an Error Code TLV with the reason code field set to 0x02 and the STA MAC address field included per section 17.2.36 in the 1905 Ack message. If the specified STA indicates support for 802.11 Beacon Report, the Multi-AP Agent shall perform the following:

- Send an 802.11 Beacon request to the STA.
- If the STA indicates support for Active and/or Passive 802.11 Beacon measurements, the Multi-AP Agent may set the Measurement Mode field in the Beacon request to Active or Passive unless an active QoS-sensitive traffic stream exists which the Multi-AP Agent expects would be unduly impacted by Active or Passive measurements, in which case Beacon Table mode may be requested.
- If the value of the SSID Length field in the query is non-zero, an SSID subelement shall be included in the 802.11 Beacon request, and shall be set to the value of the SSID field in the query. Else, an SSID subelement shall not be included.
- The Operating Class, Channel Number, BSSID and Reporting Detail fields in the Beacon Request shall be set to the corresponding values specified in the query
- If the value of the Number of AP Channel Reports field (h) in the query is greater than zero and the value of the Channel Number field in the query is 255, then h AP Channel Report subelements shall be included in the 802.11 Beacon request, each containing the specified Operating Class and Channel List.

If a Multi-AP Controller or Multi-AP Agent sends a Beacon Metrics Query message, it should aim to minimize the disruption potentially caused to the ongoing traffic of the specified STA by:

- Minimizing the number of channels on which the STA is required to scan in order to make the measurements to only those channels on which BSS of interest are operating
- Setting the Specify SSID field to one unless reports for BSS outside the currently associated ESS are required
- Refraining from setting the Reporting Detail field to value two, and minimizing the number of Element IDs requested when Reporting Detail field is set to value one

If a Multi-AP Agent receives a Beacon Report from the STA, it shall send a Beacon Metrics Response message to the Multi-AP Controller per section 17.1.23 for each Beacon Report received from the STA and include all the measurement reports contained in the Beacon Report from the STA.

If a Multi-AP Controller receives a Beacon Metrics Response message, then it shall respond within one second with a 1905 Ack message.

Note: A Measurement Report message in a Beacon Metrics Report message contains an Actual Measurement Start Time field indicating the time at which the STA performed the measurements indicated in the report. If the STA only supports Beacon Table mode (where the STA responds with cached Beacon Report measurements), it is possible that the time of this measurement will be prior to the time the Beacon Metrics Query was received by the Multi-AP Agent.

10.4 Combined infrastructure metrics

This section defines the protocol for a Multi-AP Controller to convey combined metrics regarding all the BSS and all of the backhaul links in the Multi-AP network. A Multi-AP Controller typically provides this information to Multi-AP Agents just before directing a Multi-AP Agent to perform local steering of client(s).

If triggered, a Multi-AP Controller shall send a Combined Infrastructure Metrics message per section 17.1.24 to a Multi-AP Agent. If a Multi-AP Controller sends a Combined Infrastructure Metrics message, it includes the most recently received TLVs from the corresponding Multi-AP Agents in the Multi-AP network.

If a Multi-AP Agent receives a Combined Infrastructure Metrics message, then it shall respond within one second with a 1905 Ack message.

11 Client steering

Multi-AP control messages enable efficient steering of STAs between BSSs in a Multi-AP network. These control messages enable steering of client STAs which support 802.11v BSS Transition Management (BTM) as well as client STAs which do not support BTM.

11.1 Multi-AP Controller initiated steering mandate

A Multi-AP Controller uses the Steering Mandate mechanism to mandate a Multi-AP Agent to attempt steering of one or more associated STAs.

If triggered, a Multi-AP Controller shall send a Client Steering Request message with Request Mode bit set to one indicating a Steering Mandate to a Multi-AP Agent per section 17.1.25. If the Multi-AP Agent implements Profile-1, the Multi-AP Controller shall include a Steering Request TLV into the Client Steering Request message. If the Multi-AP Agent implements Profile-2 and all the STA(s) specified in the message are Agile Multiband capable, a Multi-AP Controller that implements Profile-2 shall include a Profile-2 Steering Request TLV into the Client Steering Request message. If the Multi-AP Agent implements Profile-2 and all the STAs to be steered in the message are Agile Multiband capable, a Multi-AP Controller that implements Profile-2 shall include a Profile-2 Steering Request TLV into the Client Steering Request message. If the Multi-AP Agent implements Profile-2 and not all the STAs to be steered are Agile Multiband capable, then the Multi-AP Controller shall include a Steering Request TLV into the Client Steering Request message to steer the STAs which are not Agile Multiband capable, and a Profile-2 Steering Request TLV to steer the STAs which are Agile Multiband capable.

If a Multi-AP Agent receives a Client Steering Request message with Request Mode bit set to one, then it shall respond within one second with a 1905 Ack message. If a STA specified in the Client Steering Request message is not associated with the source BSSID specified in the same message (an error scenario), for each of those unassociated STAs, the Multi-AP Agent shall include an Error Code TLV with the reason code field set to 0x02 and the STA MAC address field included per section 17.2.36 in the 1905 Ack message.

If a Multi-AP Agent receives a Client Steering Request message with Request Mode bit set to one indicating a Steering Mandate, the Multi-AP Agent shall attempt to steer each STA identified in the request to the corresponding target BSS specified in the request message. If the Target BSSID specified for a STA in the Client Steering Request message is wildcard, the Multi-AP Agent shall attempt to steer the STA to the most suitable target BSS it has identified for that STA.

11.2 Multi-AP Controller initiated steering opportunity

A Multi-AP Controller uses the Steering Opportunity mechanism to provide a time window for a Multi-AP Agent to steer one or more associated STAs.

If triggered, a Multi-AP Controller shall send a Client Steering Request message with Request Mode bit set to zero indicating a Steering Opportunity to a Multi-AP Agent per section 17.1.25.

If a Multi-AP Controller sends a Client Steering Request message with Request Mode bit set to zero indicating a Steering Opportunity to a Multi-AP Agent, it shall not send another Client Steering Request message with Request Mode bit set to zero to the same Multi-AP Agent until the length of time indicated in the Steering Opportunity Window field of the field message has expired, or the Multi-AP Controller has received a Steering Completed message (see section 17.1.28) from the Multi-AP Agent.

If a Multi-AP Agent receives a Client Steering Request message with Request Mode bit set to zero, then it shall respond within one second with a 1905 Ack message.

If a Multi-AP Agent receives a Client Steering Request message with Request Mode bit set to zero indicating a Steering Opportunity and all the following conditions are true, the Multi-AP Agent may attempt to steer the STA(s) identified in the request to any other BSS in the Multi-AP network that the Multi-AP Agent has identified as suitable target BSS(s):

- The time delta since the message was received is less than the value of the Steering Opportunity Window field in the message
- The Multi-AP Agent has not terminated the Steering Opportunity by sending a Steering Completed message
- The STA's MAC address is not included in the Local Steering Disallowed STA List in the Steering Policy TLV

A Multi-AP Agent's decision whether or not to steer a STA and whether to steer a STA to a target BSS identified in a Client Steering Request message that indicates a Steering Opportunity should use implementation-specific mechanisms per section 11.4.

If triggered, a Multi-AP Agent shall send a Steering Completed message per section 17.1.28 to the Multi-AP Controller to terminate a Steering Opportunity. The Steering Completed message shall contain a new MID value.

If a Multi-AP Controller receives a Steering Completed message, then it shall respond within one second with a 1905 Ack message.

11.3 Multi-AP Agent initiated RCPI-based steering

A Multi-AP Controller sets the steering policy on a Multi-AP Agent using the Steering Policy TLV (see section 17.2.11).

By default, a Multi-AP Agent shall only attempt to steer a STA per the rules in sections 11.1 and 11.2. If the Multi-AP Agent receives the Steering Policy TLV, it shall additionally follow the RCPI-based steering policy rules as follows:

- If the Steering Policy field is set to 0x00 (Agent-initiated Steering Disallowed), there are no additional rules by which the Multi-AP Agent is allowed to steer a STA.
- If the Steering Policy field is set to 0x01 (Agent-initiated RCPI-based Steering Mandated) and the Multi-AP Agent indicated support for Agent-Initiated RCPI-based Steering in the AP Capability TLV, the Multi-AP Agent shall additionally follow the RCPI-based steering rules per section 11.3.1.
- If the Steering Policy field is set to 0x02 (Agent-initiated RCPI-based Steering Allowed), the Multi-AP Agent may additionally follow the RCPI-based steering rules per section 11.3.1.

11.3.1 RCPI-based steering rules

RCPI-based steering is used to allow a Multi-AP Agent to steer an associated STA to another BSS when the RCPI of the current connection becomes low.

If a Multi-AP Agent is following the RCPI-based steering rules and all of the following three conditions are true, the Multi-AP Agent attempts to steer a STA to the most suitable target BSS it has identified:

- The measured uplink RCPI for the STA falls below the RCPI Steering Threshold specified in the Steering Policy TLV for the corresponding radio.
- The STA's MAC address is not included in the Local Steering Disallowed STA List in the Steering Policy TLV.
- The Agent has identified a suitable target BSS for the STA.

11.4 Multi-AP Agent determination of target BSS

A Multi-AP Agent uses implementation-specific mechanisms to determine a suitable target BSS for a STA for steering scenarios described in sections 11.1, 11.2 and 11.3. These implementation-specific mechanisms to determine a suitable target BSS might take into account the following information:

- The most recently measured link metrics.
- Received link metrics from a STA, other Multi-AP Agents and/or the Multi-AP Controller.
- RCPI Steering Threshold and Channel Utilization Threshold specified in the most recently received Steering Policy TLV from the Multi-AP Controller.

If a Multi-AP device that implements Profile-2 receives an Association Status Notification TLV with the Association Allowance status field set to 0x00 in the most recently received Association Status Notification TLV message, then the Multi-AP device shall consider the target BSSs as not suitable for client steering.

11.5 Steering mechanisms

If a Multi-AP Agent attempts to steer a STA that indicates support for BSS Transition Management and the STA's MAC address is not included in the BTM Steering Disallowed STA list indicated in the most recently received Steering Policy TLV, the Multi-AP Agent shall:

- Transmit a BTM Request frame to the STA including a Neighbor Report element specifying the BSSID, Operating Class and Channel Number of the identified target BSS. The Operating Class shall contain an enumerated value from Table E-4 in Annex E of [1].
 - If the STA is a Wi-Fi Agile Multiband capable STA, a Multi-AP Agent that implements Profile-2 shall include in the BTM Request frame:
 - A BSS Transition Candidate Preference subelement into the Neighbor Report element and shall set the value of the Preference field in the subelement to 255 per section 3.5.2 of [8].
 - An MBO-OCE IE that contains a Transition Reason Code as specified in Table 18 of [8].
- If the steering attempt is in response to the reception of a Client Steering Request message with Request Mode bit set to one (indicating a Steering Mandate):
 - No additional Neighbor Report elements shall be included in the BTM Request frame
 - The Abridged bit in the BTM Request frame shall be set to the value of the BTM Abridged field in the Client Steering Request message received for the Steering Mandate
 - The Disassociation Imminent bit in the BTM Request frame shall be set to the value of the BTM Disassociation Imminent bit in the Client Steering Request message received for the Steering Mandate.
 - If the Disassociation Imminent bit is set to one, the Disassociation Timer field in the BTM Request frame (in TBTTs) shall be set according to the BTM Disassociation Timer field (in TUs) in the Client Steering Request message received for the Steering Mandate, else the BTM Disassociation Timer field in Client Steering Request is ignored.
 - If the Multi-AP Agent receives a BTM Response frame in response to the BTM Request frame, it shall send a Client Steering BTM Report message per section 17.1.26 containing the BTM Response to the Multi-AP Controller. The Client Steering BTM Report message shall contain a new MID value.
- If the steering attempt is in response to reception of a Multi-AP Controller initiated Steering Opportunity, the BTM Disassociation Imminent, the BTM Abridged and the BTM Disassociation Timer fields in the Client Steering Request message are ignored.

If a Multi-AP Agent attempts to steer a STA that does not indicate support for BSS Transition Management or the STA's MAC address is included in the BTM Steering Disallowed STA list indicated in the most recently received Steering Policy TLV, and:

- If the steering attempt is not in response to the reception of a Client Steering Request message with Request Mode bit set to one (indicating a Steering Mandate), the Multi-AP Agent may use the Client Association Control mechanism per section 11.6 to block the STA from associating to any BSS in the network other than the target BSS(s) and,
- If the Multi-AP Agent has not received indication that the STA has already left the BSS, the Multi-AP Agent shall send a Disassociation frame or Deauthentication frame to the STA.

If a Multi-AP Agent transmits a BTM Request frame to a STA as result of a steering attempt for a Multi-AP Controller Initiated Steering Opportunity per section 11.2 or an Agent Initiated Steering per RCPI Threshold per section 11.3, and the Multi-AP Agent subsequently identifies that the STA does not intend to leave the BSS (e.g. the STA sends a BTM Response with "Reject" status code), the Multi-AP Agent may attempt to steer the STA using the Client Association Control mechanism per section 11.6 and by sending a Disassociation frame or Deauthentication frame to the STA.

If a Multi-AP Controller receives a Client Steering BTM Report message, then it shall respond within one second with a 1905 Ack message.

11.6 Client association control mechanism

A Client Association Control Request message enables a Multi-AP Controller or a Multi-AP Agent to implicitly steer a STA (e.g. one that does not support/obey BTM requests) to a certain BSS by causing other BSS(s) in the Multi-AP network to block that STA.

If triggered, a Multi-AP Controller or a Multi-AP Agent shall send a Client Association Control Request message to a Multi-AP Agent per section 17.1.27.

If a Multi-AP Agent receives a Client Association Control Request message, then it shall respond within one second with a 1905 Ack message. If any of the STAs specified in the Client Association Control message with Association Control field set to 0x00 (indicating Client Blocking) is associated with the BSSID specified in the same message (an error scenario),

then for each of those associated STAs, the Multi-AP Agent shall include an Error Code TLV with the reason code field set to 0x01 and the STA MAC address field included per section 17.2.36 in the 1905 Ack message.

If a Multi-AP Agent receives a Client Association Control Request message with Association Control field set to 0x00 (indicating Client Blocking) and all the following conditions are true, it shall reject a first attempt by a STA specified in the request to associate to the specified BSS operated by the Multi-AP Agent and should not respond to any Probe Request frames sent by the specified STA(s) to the specified BSS:

- The time delta since the message was received is less than the value of Validity Period field in the Client Association Control Request message.
- The Multi-AP Agent has not subsequently received a Client Association Control Request message with Association Control field set to 0x01 (indicating Client Unblocking) specifying the STA.

Otherwise, the Multi-AP Agent shall not perform blocking of the STA.

A Multi-AP Agent that implements Profile-2 shall not reject associations using other association control mechanisms, such as ACL lists or (if supported) the configuration of an RSSI threshold with the RSSI based Association Rejection feature of the Wi-Fi Optimized Connectivity program (see [9]).

The Validity Period field in a Client Association Control Request message with Association Control field set to 0x01 (Client Unblocking) is ignored.

Note: When a Multi-AP Agent rejects an association attempt, it does so either by sending an Authentication frame with a “Reject” status code or, if it does not reject the authentication, by sending a (Re-)Association Response frame with a “Reject” status code.

If a Multi-AP Agent rejects an authentication request or (re-)association request as a result of having received a Client Association Control Request (i.e. if the Multi-AP Agent would have otherwise accepted the authentication or (re-)association), it shall set the Status Code in the Authentication frame or (Re-)Association Response frame to a value that does not indicate capabilities mismatch or negotiation failure, and should set the Status Code to value 33 (denied due to insufficient bandwidth) or 34 (denied due to poor channel conditions).

11.7 Wi-Fi Agile Multiband and Tunneled Message support

The fronthaul BSSs of a Multi-AP Agent shall support Wi-Fi Agile Multiband and include a Wi-Fi Agile Multiband AP Capability Indication attribute in Beacon, Probe Response, and (Re)Association Response frames as defined in [8].

If a Multi-AP Agent receives a (Re-)Association Request frame from a STA, it shall send a Tunneled message including the (Re-)Association Request frame body to the Multi-AP Controller per section 17.1.40. The Multi-AP Agent shall set the MAC address field in the Source Info TLV to be the MAC address of the STA that generated the request.

If a Multi-AP Agent receives a WNM Notification Request frame from an associated STA, it shall send a Tunneled message including the WNM Notification Request frame body to the Multi-AP Controller per section 17.1.40. The Multi-AP Agent shall set the MAC address field in the Source Info TLV to be the MAC address of the associated STA that generated the request.

If a Multi-AP Agent receives a BTM Query frame from an associated STA, it shall send a Tunneled message including the BTM Query frame body to the Multi-AP Controller per section 17.1.40. The Multi-AP Agent shall set the MAC address field in the Source Info TLV to be the MAC address of the associated STA that generated the query. The Multi-AP Agent shall also generate a BTM Request per section 3.5.1.2 of [8] to that STA.

If a Multi-AP Agent receives an ANQP request for a Neighbor Report ANQP-element from a STA, it shall send a Tunneled message including the ANQP Request frame body to the Multi-AP Controller per section 17.1.40. The Multi-AP Agent shall set the MAC address field in the Source Info TLV to be the MAC address of the STA that generated the query.

If a Multi-AP Controller receives a Tunneled message from a Multi-AP Agent, it shall respond within one second with a 1905 Ack message.

If a Multi-AP Agent cannot accept new associations in a given BSS, it shall include the MBO-OCE IE with the Association Disallowed attribute (section 4.2.4 of [9]) in Beacon and Probe Response frames and send an Association Status Notification message to the Multi-AP Controller and all the other Multi-AP Agents with the Association Allowance status

field set to 0x00. If the association status in the BSS changes, the Multi-AP Agent shall send a new Association Status Notification message.

12 Backhaul optimization

In a Multi-AP network, the backhaul STA of a Multi-AP Agent connects to a BSS to access backhaul connectivity. A Multi-AP Agent might have chosen from multiple candidate BSSs during onboarding and subsequently a Multi-AP Controller might want to move that Multi-AP Agent to a different BSS.

If triggered, a Multi-AP Controller shall send a Backhaul Steering Request message to request the Multi-AP Agent to connect its backhaul STA to a different BSS per section 17.1.29.

If a Multi-AP Agent receives a Backhaul Steering Request message, then it shall respond within one second with a 1905 Ack message to the Multi-AP Controller and attempt to (re-)associate with the target BSS specified in the message. After the Multi-AP Agent has associated with the target BSS successfully or 10 seconds has expired since the reception of the Backhaul Steering Request message, the Multi-AP Agent shall send a Backhaul Steering Response message to the Multi-AP Controller per section 17.1.30. If the Multi-AP Agent successfully associated with the target BSS specified in the Backhaul Steering Request message, the Multi-AP Agent shall set the result code in the Backhaul Steering Response TLV to 0x00.

If the Multi-AP Agent cannot (re-)associate with the target BSS specified in the Backhaul Steering Request message, the Multi-AP Agent shall set the result code in the Backhaul Steering Response TLV to 0x01 and include an Error Code TLV in the Backhaul Steering Response message with the reason code set to one of the 0x04, 0x05 and 0x06 per section 17.2.36.

In general, when a Multi-AP Agent performs the steering requested by the Multi-AP Controller, there might be a brief user data interruption on the STAs that are associated with the Multi-AP Agent due to data path change and the duration of the steering (similar to steering by using the BSS Transition Management message on a STA). If a Multi-AP Agent's fronthaul BSS is operating on the same channel as its backhaul STA and the Multi-AP Agent receives a Backhaul Steering Request message that requires the backhaul STA to switch to a different channel, there might be connection interruption on the clients that are associated with the Multi-AP Agent's fronthaul BSS while the channel switch occurs. The Multi-AP Controller should attempt to minimize or avoid such interruption if possible in such cases (e.g. by steering the clients to another fronthaul BSS, if available, prior to triggering backhaul steering).

If a Multi-AP Controller receives a Backhaul Steering Response message, then it shall respond within one second with a 1905 Ack message to the sender of the message.

12.1 Backhaul optimization by backhaul station association control

A Backhaul BSS on a Multi-AP Agent that implements Profile-2 can be configured by a Multi-AP Controller to disallow association of backhaul STAs that would result in either a Profile-1 backhaul link or a Profile-2 backhaul link. A Multi-AP Controller can configure this feature when onboarding the Multi-AP Agent, by setting bits 3 and 2 to one in the Multi-AP Extension subelement in the AP-Autoconfiguration WSC message (see section 5.2) or at any point in time by setting bit 7 and 6 to one in the Backhaul BSS Configuration TLV of a Multi-AP Policy Config Request message (see section 7.3).

If a Multi-AP Agent sets the Profile-2 bSTA Disallowed bit to one on the backhaul BSS, and receives an Association Request frame on that backhaul BSS from a backhaul STA that includes a Multi-AP Profile subelement indicating Multi-AP Profile-2, then the Multi-AP Agent shall reject the association request (see 18) on that backhaul BSS.

If a Multi-AP Agent sets the Profile-1 bSTA Disallowed bit to one on the backhaul BSS, and receives an Association Request frame on that backhaul BSS from a backhaul STA that does not include a Multi-AP Profile subelement, then the Multi-AP Agent shall reject the association request (see 18) on that backhaul BSS.

Note: When a Multi-AP Agent rejects an association attempt, it does so either by sending an Authentication frame with a "Reject" status code or, if it does not reject the authentication, by sending a (Re-)Association Response frame with a "Reject" status code.

If a Multi-AP Agent rejects an Authentication Request or (Re-)Association Request as a result of a "Backhaul STA association disallowed" configuration and it is able to provide one or more alternative backhaul BSS, it shall set the Status Code in the Authentication frame or (Re-)Association Response frame to 82 (rejected_with_suggested_bss_transition) and append at least one Neighbor Report element indicating an alternative backhaul BSS.

If a Multi-AP Agent rejects an authentication request or (re-)association request as a result of a “Backhaul STA association disallowed” configuration and it is not able to provide a suggested BSS transition target, it shall set the Status Code in the corresponding Authentication frame or (Re-)Association Response frame to 12 (denied other reasons).

A Multi-AP Controller that implements Profile-2 should not request a Multi-AP Agent that implements Profile-1 to associate its backhaul STA to a BSS configured as “Profile-1 Backhaul STA association disallowed”.

A Multi-AP Controller that implements Profile-2 should not request a Multi-AP Agent that implements Profile-2 to associate its backhaul STA to a BSS configured as “Profile-2 Backhaul STA association disallowed”.

13 Multi-AP messaging security

This specification utilizes multiple security layers.

A Multi-AP device wishing to join a network of Multi-AP devices satisfies the onboarding authentication of its network connectivity. For example, Wi-Fi connectivity uses WPA2-Personal.

Multi-AP 1905 layer messaging is protected against out-of-network eavesdropping through utilization of encryption feature(s) of its underlying network connectivity. A Multi-AP interface is considered authenticated when the underlying networking technology encryption mode has been successfully configured.

For configuration of messaging for Multi-AP Agent credentials related to a BSS, the Wi-Fi Simple Configuration V2 mechanism (see section 7.1 of [5]) is used as a further layer of protection against unauthorized access and disclosure.

14 Four-address MAC header format

The address handling description applies immediately after a Multi-AP Agent has connected to a Multi-AP network using an onboarding method per section 5.

14.1 Wi-Fi backhaul frame and address handling

If a Multi-AP device receives a Multi-AP IE from another Multi-AP device, then thereafter a Multi-AP device frame formats shall be compliant with section 9 of [1] with the following exceptions:

14.1.1 Receiver requirements

If source address (SA field) has the same value as the IEEE MAC individual address of the backhaul STA (TA field), a Fronthaul AP shall support receiving both Four-Address and Three-Address MAC header format Data frames from a backhaul STA.

If source address (SA field) has a different value than the IEEE MAC individual address of the backhaul STA (TA field), a Fronthaul AP shall support receiving Four-Address header format Data frames from a backhaul STA.

If destination address (DA field) has the same value as the IEEE MAC individual address of the backhaul STA (RA field), a backhaul STA shall support receiving both Four-Address and Three-Address MAC header format Data frames from a Fronthaul AP.

If destination address (DA field) has a different value than the IEEE MAC individual address of the backhaul STA (RA field), a backhaul STA shall support receiving Four-Address MAC header format Data frames from a Fronthaul AP.

14.1.2 Transmitter requirements

If a backhaul STA sends a Data frame to an associated Fronthaul AP with a source address (SA field) different from the IEEE MAC individual address of the backhaul STA, then the backhaul STA shall set the To DS B8 field to one and From DS B9 field to one in the MAC Frame Control field, per section 9.2.4.1 of [1].

If a backhaul STA sends a Data frame to an associated Fronthaul AP with a source address (SA field) same as the IEEE MAC individual address of the backhaul STA, then the backhaul STA shall either:

- Follow the Three-Address MAC header procedures of [1], or
- Set the To DS B8 field to one and From DS B9 field to one in the MAC Frame Control field, per section 9.2.4.1 of [1].

The backhaul STA shall set the RA field ("Address 1" (per Table 9-26 of [1])) in the Data frame sent over the backhaul link to the IEEE MAC individual address of the AP or group address. The backhaul STA shall set the TA field ("Address 2" (per Table 9-26 of [1])) in the Data frame sent over the backhaul link to the IEEE MAC individual address of the Backhaul STA.

If a Fronthaul AP sends a Data frame to an associated backhaul STA with a destination address (DA field) different from the IEEE MAC individual address of the backhaul STA, then the Fronthaul AP shall set the To DS B8 field to one and From DS B9 field to one in the MAC Frame Control field, per section 9.2.4.1 of [1].

If a Fronthaul AP sends a Data frame to an associated backhaul STA with a destination address (DA field) same as the IEEE MAC individual address of the backhaul STA, then the Fronthaul AP shall either:

- Follow the Three-Address MAC header procedures of [1], or
- Set the To DS B8 field to one and From DS B9 field to one in the MAC Frame Control field, per section 9.2.4.1 of [1].

The Fronthaul AP shall set the RA field ("Address 1" (per Table 9-26 of [1])) in the Data frame sent over the backhaul link to the IEEE MAC individual address of the backhaul STA or group address. The Fronthaul AP shall set the TA field ("Address 2" (per Table 9-26 of [1])) in the Data frame sent over the backhaul link to the IEEE MAC individual address of the Fronthaul AP.

14.1.3 Wired backhaul frame and address handling

Data frames shall be carried with Ethernet frames and handled per section 3 of [3].

15 Multi-AP control messaging reliability

All Multi-AP control messages sent using the CMDU unicast transmission procedure rely on a paired transaction to provide reliability. Many Multi-AP control messages are request and response message pairs e.g. Client Capability Query message and Client Capability Report message. For Multi-AP control messages that are sent as unicast notifications without an expected information response, a generic 1905 Ack message is sent per section 17.1.32. The generic 1905 Ack message shall contain the same MID that was received in the Multi-AP control message that this Ack message is acknowledging.

To improve reliability, if the request message and/or the response message is lost, the sender may send another request message (using a new MID value). Similarly, if the notification message and/or the 1905 Ack message is lost, the sender may send another notification message (using a new MID value).

A new transmission type and the corresponding procedures are defined in section 15.1 to increase the reliability of a message defined in [2] sent using the CMDU relayed multicast transmission procedure. Its applicability to each message is described in Table 9.

15.1 CMDU reliable multicast transmission

Since the messages sent by the CMDU relayed multicast transmission procedure do not return an acknowledgement, in some extreme poor link condition (e.g. very high packet error probability condition) the CMDU might be lost. To increase the probability of receiving the CMDUs, a Multi-AP device sends the CMDU as relayed multicast and also sends the same CMDU (with the same MID) using the unicast procedure to other discovered Multi-AP devices. A receiver discards any duplicated received CMDU based on the MID.

15.1.1 CMDU reliable multicast transmission procedures

In the CMDU reliable multicast transmission procedures,

- the Multi-AP device shall transmit the CMDU as a relayed multicast transmission per section 7.3 of [2] (i.e. with the relayIndicator field in the CMDU set to one).
- the Multi-AP device shall transmit the same CMDU as a unicast transmission (using the same MID but with the relayIndicator field in the CMDU set to zero) per section 7.4 of [2] to other discovered Multi-AP devices on the Multi-AP network.

15.1.2 CMDU reliable multicast reception procedures

In the CMDU reliable multicast reception procedures,

- the Multi-AP device shall process a received CMDU with the relayIndicator set to one per section 7.6 of [2].
- the Multi-AP device shall process a received CMDU with the relayIndicator set to zero per section 7.7 of [2].

16 Higher layer data payload over 1905

Multi-AP control messages are defined to provide a generic mechanism to carry higher layer data as opaque payload over the 1905 abstraction layer. This generic mechanism can be used to transport higher layer protocol messages over 1905 on a Multi-AP device, e.g. transport higher layer messages to access and manipulate TR-181 data objects (see [4]).

If triggered by an HLE, a Multi-AP Controller or a Multi-AP Agent shall send a Higher Layer Data message per section 17.1.31. A Multi-AP Controller or a Multi-AP Agent shall include a Higher Layer Data TLV received from the HLE in the Higher Layer Data message.

If a Multi-AP Controller or a Multi-AP Agent receives a Higher Layer Data message, then it shall respond within one second with a 1905 Ack message per section 17.1.32. The 1905 Ack message shall contain the same MID that was received in the Higher Layer Data message.

17 Multi-AP control messaging

Multi-AP control messages are carried using the 1905 CMDU format as defined in [2]. The 1905 CMDU header includes a Message Type field identifying the type of the message carried in the CMDU. 1905 Message Type values from the reserved space are used for Multi-AP control messages. Multi-AP specific TLVs are defined using the 1905 tlvType value range. A Multi-AP device that implements Profile-2 shall only include the End of Message TLV in the last fragment of a CMDU (when lastFragmentIndicator is set to one).

17.1 Multi-AP message format

This section defines the message formats for Multi-AP control messages and those 1905 control messages defined in 1905 which are extended for Multi-AP support.

The first column of Table 9 shows the Multi-AP Profile (see 18) for which the message was originally introduced or extended from 1905. The second column of Table 9 shows the latest Multi-AP Profile for which the message was modified.

Table 9. Message types

Introduced in Multi-AP Profile	Last modified in Multi-AP Profile	Message type	Protocol	Value	Transmission type	Relay indicator field	Use CMDU Reliable Multicast?	Description
1	1	1905 Topology Notification message	STA capability	0x0001	Reliable multicast	See 15.1	Yes	A message to notify that a device's 1905 topology entries have changed.
1	2	1905 Topology Query message	Topology discovery	0x0002	Unicast	0	No	A message to query a Multi-AP Agent for its topology information.
1	2	1905 Topology Response message	STA capability	0x0003	Unicast	0	No	A message to carry topology information in response to a topology query.
1	2	1905 AP- Autoconfiguration Search message	AP configuration	0x0007	Relayed multicast	1	No	A message to search for the Controller.
1	2	1905 AP- Autoconfiguration Response message	AP configuration	0x0008	Unicast	0	No	A message to answer to a 1905 AP- Autoconfiguration Search message.
1	2	1905 AP- Autoconfiguration WSC message	AP configuration	0x0009	Unicast	0	No	A message to carry a WSC registration frame.
1	1	1905 Ack message	1905 CMDU	0x8000	Unicast	0	No	A message to acknowledge certain 1905 messages.
1	1	AP Capability Query message	AP capability	0x8001	Unicast	0	No	A message to query a fronthaul

Introduced in Multi-AP Profile	Last modified in Multi-AP Profile	Message type	Protocol	Value	Transmission type	Relay indicator field	Use CMDU Reliable Multicast?	Description
								AP's capability information.
1	2	AP Capability Report message	AP capability	0x8002	Unicast	0	No	A message to report a fronthaul AP's capability information.
1	2	Multi-AP Policy Config Request message	Multi-AP configuration	0x8003	Unicast	0	No	A message to configure Multi-AP control related policies.
1	1	Channel Preference Query message	Channel Selection	0x8004	Unicast	0	No	A message to query operating channel preferences for AP radios of Multi-AP Agents.
1	2	Channel Preference Report message	Channel Selection	0x8005	Unicast	0	No	A message to report operating channel preferences for AP radios of Multi-AP Agents.
1	1	Channel Selection Request message	Channel Selection	0x8006	Unicast	0	No	A message to send channel selection configurations for AP radios of Multi-AP Agents.
1	1	Channel Selection Response message	Channel Selection	0x8007	Unicast	0	No	A message to report the Multi-AP Agent's response to the Channel Selection request.
1	1	Operating Channel Report message	Channel Selection	0x8008	Unicast	0	No	A message to report the current operating channel configurations for AP radios of Multi-AP Agents.
1	1	Client Capability Query message	STA capability	0x8009	Unicast	0	No	A message to query a client's capability information.
1	1	Client Capability Report message	STA capability	0x800A	Unicast	0	No	A message to report a client's capability information.
1	2	AP Metrics Query Message	Link metric collection	0x800B	Unicast	0	No	A message to query an AP's metrics.

Introduced in Multi-AP Profile	Last modified in Multi-AP Profile	Message type	Protocol	Value	Transmission type	Relay indicator field	Use CMDU Reliable Multicast?	Description
1	2	AP Metrics Response message	Link metric collection	0x800C	Unicast	0	No	A message to report an AP's metric.
1	1	Associated STA Link Metrics Query message	Link metric collection	0x800D	Unicast	0	No	A message to query an associated STA's link metrics.
1	2	Associated STA Link Metrics Response message	Link metric collection	0x800E	Unicast	0	No	A message to report an associated STA's link metrics.
1	1	Unassociated STA Link Metrics Query message	Link metric collection	0x800F	Unicast	0	No	A message to query an unassociated STA's link metrics.
1	1	Unassociated STA Link Metrics Response message	Link metric collection	0x8010	Unicast	0	No	A message to report an unassociated STA's link metrics.
1	1	Beacon Metrics Query message	Link metric collection	0x8011	Unicast	0	No	A message to query the Beacon frame metrics.
1	1	Beacon Metrics Response message	Link metric collection	0x8012	Unicast	0	No	A message to report the Beacon frame metrics.
1	1	Combined Infrastructure Metrics message	Link metric collection	0x8013	Unicast	0	No	A message to send combined infrastructure metrics.
1	2	Client Steering Request message	Client Steering	0x8014	Unicast	0	No	A message to trigger steering for one or more STAs.
1	1	Client Steering BTM Report message	Client Steering	0x8015	Unicast	0	No	A message to provide BTM report received from a STA.
1	1	Client Association Control Request message	Client Steering	0x8016	Unicast	0	No	A message to enable blocking of STA(s) association on Multi-AP Agent.
1	1	Steering Completed message	Client Steering	0x8017	Unicast	0	No	A message to provide indication of termination of a Steering Opportunity

Introduced in Multi-AP Profile	Last modified in Multi-AP Profile	Message type	Protocol	Value	Transmission type	Relay indicator field	Use CMDU Reliable Multicast?	Description
1	1	Higher Layer Data message	Higher layer data payload	0x8018	Unicast	0	No	A message to query a client's capability information.
1	1	Backhaul Steering Request message	Backhaul optimization	0x8019	Unicast	0	No	A message to steer a backhaul STA.
1	1	Backhaul Steering Response message	Backhaul optimization	0x801A	Unicast	0	No	A message to respond to the Backhaul Steering Request message
2	2	Channel Scan Request message	Channel scan	0x801B	Unicast	0	No	A message to request a channel scan.
2	2	Channel Scan Report message	Channel scan	0x801C	Unicast	0	No	A message to report the channel scan result.
2	2	CAC Request message	DFS CAC	0x8020	Unicast	0	No	A message to request a DFS CAC.
2	2	CAC Termination message	DFS CAC	0x8021	Unicast	0	No	A message to terminate a DFS CAC.
2	2	Client Disassociation Stats message	Data Element	0x8022	Unicast	0	No	A message to report disassociated client's stats
2	2	Error Response message	Traffic Separation	0x8024	Unicast	0	No	A message to report an error pertaining to traffic separation request.
2	2	Association Status Notification message	Client steering	0x8025	Reliable multicast	0	Yes	A message notifying Controller that a Multi-AP Agent cannot accept associations from client devices
2	2	Tunneled message	Tunnel	0x8026	Unicast	0	No	A message relaying from Multi-AP Agent to Controller the frame body without the MAC header of an 802.11 frame received by the Agent from a STA.

Introduced in Multi-AP Profile	Last modified in Multi-AP Profile	Message type	Protocol	Value	Transmission type	Relay indicator field	Use CMDU Reliable Multicast?	Description
2	2	Backhaul STA Capability Query message	Backhaul STA capability	0x8027	Unicast	0	No	A message to query the Backhaul STA capability of the Multi-AP Agent.
2	2	Backhaul STA Capability Report message	Backhaul STA capability	0x8028	Unicast	0	No	A message to respond to the Backhaul STA Capability Query message.
2	2	Failed Connection message	Data Element	0x8033	Unicast	0	No	A message to report failed connection.

Note: the notation "[Profile-2]" in the messages' definition in the reminder of this section denotes TLVs that are mandatory, conditionally present or optional when the transmitter implements Profile-2, as detailed in this specification. The lack of such notation indicates TLVs that are mandatory, conditionally present or optional for any Multi-AP device.

Table 10 summarizes the content of each message as per the Multi-AP device's profile. It is reminded that, as per [2], a Multi-AP device that implements a certain Profile ignores any TLV that is not specified by such Profile for the type of message received. A Multi-AP device ignores the entire message if the message does not include all of the mandatory TLVs that are listed for this message as per the Profile of the transmitter (when known) or if there is no Multi-AP Profile for which such message would be valid (when transmitter's Profile is unknown).

Table 10. Message Content by Profile

Message type	Value	Multi-AP device implements	
		Profile 1	Profile-2
1905 Topology Notification	0x0001	One 1905.1 AL MAC address type TLV ([2]) Zero or One Client Association Event TLV (17.2.20)	
1905 Topology Query	0x0002	No TLVs	One Multi-AP Profile TLV (17.2.47)
1905 Topology Response	0x0003	One device information type TLV ([2]) Zero or more device bridging capability TLVs ([2]) Zero or more non-1905 neighbor device list TLVs ([2]) Zero or more 1905.1 neighbor device TLVs ([2]) Zero or one SupportedService TLV (17.2.1) One AP Operational BSS TLV (17.2.4) Zero or one Associated Clients TLV (17.2.5)	
			One Multi-AP Profile TLV (17.2.47)
1905 AP-Autoconfiguration Search	0x0007	One 1905.1 AL MAC address type TLV ([2]) One SearchedRole TLV ([2]) One AutoconfigFreqBand TLV ([2]) Zero or one SupportedService TLV (17.2.1) Zero or one SearchedService TLV (17.2.2)	
			One Multi-AP Profile TLV (17.2.47)
1905 AP-Autoconfiguration Response	0x0008	One SupportedRole TLV ([2]) One SupportedFreqBand TLV ([2]) Zero or one SupportedService TLV (17.2.1)	
			One Multi-AP Profile TLV (17.2.47)

Message type	Value	Multi-AP device implements	
		Profile 1	Profile-2
1905 AP-Autoconfiguration WSC sent by a Multi-AP Agent	0x0009	One AP Radio Basic Capabilities TLV (17.2.7) One WSC TLV (containing M1) ([2])	
			One Profile-2 AP Capability TLV (17.2.48) One AP Radio Advanced Capabilities TLV (17.2.52)
1905 AP-Autoconfiguration WSC sent by a Multi-AP Controller	0x0009	One AP Radio Identifier TLV (17.2.3). One or more WSC TLV (containing M2) ([2])	
			Zero or one Default 802.1Q Settings TLV (17.2.49) Zero or one Traffic Separation Policy TLV (17.2.50)
1905 Ack	0x8000	Zero or more Error Code TLVs (17.2.36)	
AP Capability Query	0x8001	No TLVs are required in this message	
AP Capability Report	0x8002	One AP Capability TLV (17.2.6). One or more AP Radio Basic Capabilities TLV (17.2.7). Zero or more AP HT Capabilities TLV (17.2.8). Zero or more AP VHT Capabilities TLV (17.2.9). Zero or more AP HE Capabilities TLV (17.2.10).	
			One Channel Scan Capabilities TLV (17.2.38) One CAC Capabilities TLV (17.2.46) One Profile-2 AP Capability TLV (17.2.48) One Metric Collection Interval TLV (17.2.59)
Multi-AP Policy Config Request	0x8003	Zero or one Steering Policy TLV (17.2.11) Zero or one Metric Reporting Policy TLV (17.2.12)	
			Zero or one Default 802.1Q Settings TLV (17.2.49) Zero or one Traffic Separation Policy TLV (17.2.50) Zero or one Channel Scan Reporting Policy TLV (17.2.37) Zero or one Unsuccessful Association Policy TLV (17.2.58) Zero or more Backhaul BSS Configuration TLV (17.2.66)
Channel Preference Query	0x8004	No TLVs are required in this message	
Channel Preference Report	0x8005	Zero or more Channel Preference TLVs (17.2.13) Zero or more Radio Operation Restriction TLVs (17.2.14)	
			Zero or one CAC Completion Report TLV (17.2.44) One CAC Status Report TLV (17.2.45)
Channel Selection Request	0x8006	Zero or more Channel Preference TLVs (17.2.13) Zero or more Transmit Power Limit TLVs (17.2.15)	
Channel Selection Response	0x8007	One or more Channel Selection Response TLVs (17.2.16)	
Operating Channel Report	0x8008	One or more Operating Channel Report TLVs (17.2.17)	
Client Capability Query	0x8009	One Client Info TLV (17.2.18)	
Client Capability Report	0x800A	One Client Info TLV (17.2.18) One Client Capability Report TLV (17.2.19) Zero or one Error Code TLV (17.2.36)	
AP Metrics Query	0x800B	One AP metric query TLV (17.2.21)	
			Zero or more AP Radio Identifier TLVs (17.2.3)
AP Metrics Response	0x800C	One or more AP Metrics TLVs (17.2.22) Zero or more Associated STA Traffic Stats TLVs (17.2.35)	

Message type	Value	Multi-AP device implements	
		Profile 1	Profile-2
		Zero or more Associated STA Link Metrics TLVs (17.2.24)	
			One or more AP Extended Metrics TLVs (17.2.61) Zero or more Radio Metrics TLVs (17.2.60) Zero or more Associated STA Extended Link Metrics TLVs (17.2.62)
Associated STA Link Metrics Query	0x800D	One STA MAC Address type TLV (17.2.23)	
Associated STA Link Metrics Response	0x800E	One or more Associated STA Link Metrics TLVs (17.2.24) Zero or one Error Code TLV (17.2.36)	
			One or more Associated STA Extended Link Metrics TLVs (17.2.62)
Unassociated STA Link Metrics Query	0x800F	One Unassociated STA Link Metrics query TLV (17.2.25)	
Unassociated STA Link Metrics Response	0x8010	One Unassociated STA Link Metrics response TLV (17.2.26)	
Beacon Metrics Query	0x8011	One Beacon metrics query TLV (17.2.27)	
Beacon Metrics Response	0x8012	One Beacon metrics response TLV (17.2.28)	
Combined Infrastructure Metrics	0x8013	One AP Metrics TLV (17.2.22) for each BSS the Controller determines to provide the AP Metrics information. For each backhaul link (between two Multi-AP Agents) in the network: One 1905 transmitter link metric TLV ([2]) corresponding to the backhaul AP. One 1905 transmitter link metric TLV ([2]) corresponding to the backhaul STA. One 1905 receiver link metric TLV ([2]) corresponding to the backhaul AP. One 1905 receiver link metric TLV ([2]) corresponding to the backhaul STA.	
Client Steering Request	0x8014	One Steering Request TLV (17.2.29)	If the message is sent to a Multi-AP Agent that implements Profile-1: One Steering Request TLV (17.2.29) If the message is sent to a Multi-AP Agent that implements Profile-2: Zero or one Steering Request TLV (17.2.29) to non-Agile Multiband capable STAs. Zero or one Profile-2 Steering Request TLV (17.2.56) to Agile Multiband capable STAs.
Client Steering BTM Report	0x8015	One Steering BTM Report TLV (17.2.30)	
Client Association Control Request	0x8016	One or more Client Association Control Request TLVs (17.2.31)	
Steering Completed	0x8017	No TLVs are required in this message.	
Higher Layer Data	0x8018	One Higher Layer Data TLV (17.2.34)	
Backhaul Steering Request	0x8019	One Backhaul Steering Request TLV (17.2.32)	
Backhaul Steering Response	0x801A	One Backhaul Steering Response TLV (17.2.33) Zero or one Error Code TLV (17.2.36).	
Channel Scan Request	0x801B		One Channel Scan Request TLV (17.2.39)
Channel Scan Report	0x801C		One Timestamp TLV (17.2.41) One or more Channel Scan Result TLVs (17.2.40)
CAC Request	0x8020		One CAC Request TLV (17.2.42)
CAC Termination	0x8021		One CAC Termination TLV (17.2.43)
Client Disassociation Stats	0x8022		One STA MAC Address TLV (17.2.23) One Reason Code TLV (17.2.64) One Associated STA Traffic Stats TLV (17.2.35)
Error Response	0x8024		One or more Profile-2 Error Code TLV (17.2.51)

Message type	Value	Multi-AP device implements	
		Profile 1	Profile-2
Association Status Notification	0x8025		One Association Status Notification TLVs (17.2.53)
Tunneled	0x8026		Source Info TLV (17.2.54). Tunneled message type TLV (17.2.55) One or more Tunneled TLVs (17.2.56)
Backhaul STA Capability Query	0x8027		No TLVs are required in this message
Backhaul STA Capability Report	0x8028		Zero or more Backhaul STA Radio Capabilities TLV (17.2.65)
Failed Connection	0x8033		One STA MAC Address Type TLV (17.2.23) One Status Code TLV (17.2.63) Zero or one Reason Code TLV (17.2.64).

17.1.1 1905 AP-Autoconfiguration Search message format (extended)

The following TLVs shall also be included in this message, in addition to TLVs listed in [2]:

- Zero or one SupportedService TLV (see section 17.2.1).
- Zero or one SearchedService TLV (see section 17.2.2).
- One Multi-AP Profile TLV (see section 17.2.47). [Profile-2]

17.1.2 1905 AP-Autoconfiguration Response message format (extended)

The following TLV shall also be included in this message, in addition to TLVs listed in [2]

- Zero or one SupportedService TLV (see section 17.2.1).
- One Multi-AP Profile TLV (see section 17.2.47). [Profile-2]

17.1.3 1905 AP-Autoconfiguration WSC message format (extended)

The following TLVs shall also be included in this message:

- If the message is sent by the Multi-AP Agent:
 - One AP Radio Basic Capabilities TLV (see section 17.2.7).
 - One WSC TLV (containing M1).
 - One Profile-2 AP Capability TLV (see section 17.2.48) [Profile-2]
 - One AP Radio Advanced Capabilities TLV (see section 17.2.52). [Profile-2]
- If the message is sent by the Multi-AP Controller:
 - One AP Radio Identifier TLV (see section 17.2.3).
 - One or more WSC TLV (containing M2).
 - Zero or one Default 802.1Q Settings TLV (see section 17.2.49). [Profile-2]
 - Zero or one Traffic Separation Policy TLV (see section 17.2.50). [Profile-2]

17.1.4 1905 Topology Response message format (extended)

The following TLV shall also be included in this message, in addition to TLVs listed [2]:

- Zero or one SupportedService TLV (see section 17.2.1).
- One AP Operational BSS TLV (see section 17.2.4).
- Zero or one Associated Clients TLV (see section 17.2.5).
- One Multi-AP Profile TLV (see section 17.2.47). [Profile-2]

17.1.5 1905 Topology Notification message format (extended)

The following TLV shall also be included in the 1905 Topology Notification message:

- Zero or one Client Association Event TLV (see section 17.2.20).

17.1.6 AP Capability Query message format

No TLVs are required in this message.

17.1.7 AP Capability Report message format

The following TLVs shall be included in this message:

- One AP Capability TLV (see section 17.2.6).
- One or more AP Radio Basic Capabilities TLV (see section 17.2.7).
- Zero or more AP HT Capabilities TLV (see section 17.2.8).
- Zero or more AP VHT Capabilities TLV (see section 17.2.9).
- Zero or more AP HE Capabilities TLV (see section 17.2.10).
- One Channel Scan Capabilities TLV (see section 17.2.38) [Profile-2]
- One CAC Capabilities TLV (see section 17.2.46). [Profile-2]
- One Profile-2 AP Capability TLV (see section 17.2.48). [Profile-2]
- One Metric Collection Interval TLV (see section 17.2.59). [Profile-2]

17.1.8 Multi-AP Policy Config Request message format

The following TLV shall be included in this message:

- Zero or one Steering Policy TLV (see section 17.2.11).
- Zero or one Metric Reporting Policy TLV (see section 17.2.12).
- Zero or one Default 802.1Q Settings TLV (see section 17.2.49). [Profile-2]
- Zero or one Traffic Separation Policy TLV (see section 17.2.50). [Profile-2]
- Zero or one Channel Scan Reporting Policy TLV (see section 17.2.37). [Profile-2]
- Zero or one Unsuccessful Association Policy TLV (see section 17.2.58). [Profile-2]
- Zero or more Backhaul BSS Configuration TLV (see section 17.2.66). [Profile-2]

17.1.9 Channel Preference Query message format

No TLVs are required in this message.

17.1.10 Channel Preference Report message format

The following TLVs shall be included in this message:

- Zero or more Channel Preference TLVs (see section 17.2.13).
- Zero or more Radio Operation Restriction TLVs (see section 17.2.14).
- Zero or one CAC Completion Report TLV (see section 17.2.44). [Profile-2]
- One CAC Status Report TLV (see section 17.2.45). [Profile-2]

17.1.11 Channel Selection Request message format

The following TLVs shall be included in this message:

- Zero or more Channel Preference TLVs (see section 17.2.13).
- Zero or more Transmit Power Limit TLVs (see section 17.2.15).

17.1.12 Channel Selection Response message format

The following TLVs shall be included in this message:

- One or more Channel Selection Response TLVs (see section 17.2.16).

17.1.13 Operating Channel Report message format

The following TLVs shall be included in this message:

- One or more Operating Channel Report TLVs (see section 17.2.17).

17.1.14 Client Capability Query message format

The following TLV shall be included in this message:

- One Client Info TLV (see section 17.2.18).

17.1.15 Client Capability Report message format

The following TLVs shall be included in this message:

- One Client Info TLV (see section 17.2.18).
- One Client Capability Report TLV (see section 17.2.19).
- Zero or one Error Code TLV (see section 17.2.36).

17.1.16 AP Metrics Query Message format

The following TLVs shall be included in this message:

- One AP metric query TLV (see section 17.2.21).
- Zero or more AP Radio Identifier TLVs (see section 17.2.3). [Profile-2]

17.1.17 AP Metrics Response Message format

The following TLVs shall be included in this message:

- One or more AP Metrics TLVs (see section 17.2.22).
- One or more AP Extended Metrics TLVs (see section 17.2.61) [Profile-2]
- Zero or more Radio Metrics TLVs (see section 17.2.60) [Profile-2]
- Zero or more Associated STA Traffic Stats TLVs (see section 17.2.35).
- Zero or more Associated STA Link Metrics TLVs (see section 17.2.24).
- Zero or more Associated STA Extended Link Metrics TLVs (see section 17.2.62) [Profile-2]

17.1.18 Associated STA Link Metrics Query message format

The following TLVs shall be included in this message:

- One STA MAC Address type TLV (see section 17.2.23).

17.1.19 Associated STA Link Metrics Response message format

The following TLVs shall be included in this message:

- One or more Associated STA Link Metrics TLVs (see section 17.2.24).
- Zero or one Error Code TLV (see section 17.2.36).
- One or more Associated STA Extended Link Metrics TLVs (see section 17.2.62) [Profile-2]

17.1.20 Unassociated STA Link Metrics Query message format

The following TLVs shall be included in this message:

- One Unassociated STA Link Metrics query TLV (see section 17.2.25).

17.1.21 Unassociated STA Link Metrics Response message format

The following TLVs shall be included in this message:

- One Unassociated STA Link Metrics response TLV (see section 17.2.26).

17.1.22 Beacon Metrics Query message format

The following TLVs shall be included in this message:

- One Beacon metrics query TLV (see section 17.2.27).

17.1.23 Beacon Metrics Response message format

The following TLVs shall be included in this message:

- One Beacon metrics response TLV (see section 17.2.28).

17.1.24 Combined Infrastructure Metrics message format

The following TLVs shall be included in this message:

- One AP Metrics TLV (see section 17.2.22) for each BSS the Controller determines to provide the AP Metrics information.
- For each backhaul link (between two Multi-AP Agents) in the network:
 - One 1905 transmitter link metric TLV (see 6.4.11 of [2]) corresponding to the backhaul AP.
 - One 1905 transmitter link metric TLV (see 6.4.11 of [2]) corresponding to the backhaul STA.
 - One 1905 receiver link metric TLV (see 6.4.12 of [2]) corresponding to the backhaul AP.
 - One 1905 receiver link metric TLV (see 6.4.12 of [2]) corresponding to the backhaul STA.

17.1.25 Client Steering Request message format

The following TLV shall be included in this message:

- If the message is sent to a Multi-AP Agent that implements only Profile-1 or is sent from a Multi-AP device that implements Profile-1:
 - One Steering Request TLV (see section 17.2.29).
- If the message is sent to a Multi-AP Agent that implements Profile-2 from a Multi-AP device that implements only Profile-2:
 - Zero or one Steering Request TLV (see section 17.2.29) to non-Agile Multiband capable STAs.
 - Zero or one Profile-2 Steering Request TLV (see section 17.2.57). to Agile Multiband capable STAs.

17.1.26 Client Steering BTM Report message format

The following TLV shall be included in this message:

- One Steering BTM Report TLV (see section 17.2.30).

17.1.27 Client Association Control Request message format

The following TLV shall be included in this message:

- One or more Client Association Control Request TLVs (see section 17.2.31).

17.1.28 Steering Completed message format

No TLVs are required in this message.

17.1.29 Backhaul Steering Request message format

The following TLV shall be included in this message:

- One Backhaul Steering Request TLV (see section 17.2.32).

17.1.30 Backhaul Steering Response message format

The following TLV shall be included in this message:

- One Backhaul Steering Response TLV (see section 17.2.33).
- Zero or one Error Code TLV (see section 17.2.36).

17.1.31 Higher Layer Data message format

The following TLV shall be included in this message:

- One Higher Layer Data TLV (see section 17.2.34).

17.1.32 1905 Ack message format

The following TLV shall be included in this message:

- Zero or more Error Code TLVs (see section 17.2.36).

17.1.33 Channel Scan Request message format

The following TLV shall be included in this message:

- One Channel Scan Request TLV (see 17.2.39).

17.1.34 Channel Scan Report message format

The following TLV shall be included in this message:

- One Timestamp TLV (see 17.2.41).
- One or more Channel Scan Result TLVs (see 17.2.40).

17.1.35 CAC Request message format

The following TLV shall be included in this message:

- One CAC Request TLV (see section 17.2.42).

17.1.36 CAC Termination message format

The following TLV shall be included in this message:

- One CAC Termination TLV (see section 17.2.43).

17.1.37 Error Response message format

The following TLV shall be included in this message:

- One or more Profile-2 Error Code TLV (see 17.2.51).

17.1.38 Topology Query message format

The following TLV shall be included in this message:

- One Multi-AP Profile TLV (see section 17.2.47). [Profile-2]

17.1.39 Association Status Notification message format

The following TLVs shall be included in this message:

- One Association Status Notification TLVs (see section 17.2.53).

17.1.40 Tunneled message format

The following TLVs shall be included in this message:

- One Source Info TLV (see section 17.2.54).
- One Tunneled message type TLV (see section 17.2.55).
- One or more Tunneled TLVs (see section 17.2.56).

17.1.41 Client Disassociation Stats message format

The following TLVs shall be included in this message:

- One STA MAC Address TLV (See section 17.2.23)
- One Reason Code TLV (see section 17.2.64)
- One Associated STA Traffic Stats TLV (see section 17.2.35)

17.1.42 Backhaul STA Capability Query message format

No TLVs are required in this message.

17.1.43 Backhaul STA Capability Report message format

The following TLVs shall be included in this message:

- Zero or more Backhaul STA Radio Capabilities TLV (see section 17.2.65).

17.1.44 Failed Connection message

The following TLVs shall be included in this message:

- One STA MAC Address Type TLV (see 17.2.23)
- One Status Code TLV (see 17.2.63)
- Zero or one Reason Code TLV (see 17.2.64).

17.2 Multi-AP TLVs format

This section defines the format for the Multi-AP specific TLVs.

17.2.1 SupportedService TLV format

Table 11 provides the definition for the SupportedService TLV.

Table 11. SupportedService TLV format

Field	Length	Value	Description
tlvType	1 octet	0x80	Supported service information TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	k	List of supported service(s).
	1 octet	0x00: Multi-AP Controller 0x01: Multi-AP Agent 0x02 – 0xFF: Reserved	Supported service.
	The above field is repeated k – 1 times.		

17.2.2 SearchedService TLV format

Table 12 provides the definition for the SearchedService TLV.

Table 12. SearchedService TLV format

Field	Length	Value	Description
tlvType	1 octet	0x81	Searched service information TLV.
tlvLength	2 octets	variable	Number of octets in ensuing field.
tlvValue	1 octet	k	List of searched service(s).
	1 octet	0x00: Multi-AP Controller 0x01 – 0xFF: Reserved	Searched service.
	The above field is repeated k – 1 times.		

17.2.3 AP Radio Identifier TLV format

Table 13 provides the definition for the AP Radio Identifier TLV.

Table 13. AP Radio Identifier TLV format

Field	Length	Value	Description
tlvType	1 octet	0x82	AP Radio Identifier TLV.
tlvLength	2 octets	6	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique Identifier of a radio of the Multi-AP Agent.

17.2.4 AP Operational BSS TLV format

Table 14 provides the definition for the AP Operational BSS TLV.

Table 14. AP Operational BSS TLV format

Field	Length	Value	Description
tlvType	1 octet	0x83	AP Operational BSS TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	k	Number of radios reported.
	6 octets	Variable	Radio Unique Identifier of a radio.
	1 octet	m	Number of BSS (802.11 Local interfaces) currently operating on the radio.
	6 octets	Variable	MAC Address of Local Interface (equal to BSSID) operating on the radio.
	1 octet	n	SSID length.
	n octets	Variable	SSID
	The above 3 fields are repeated m – 1 times (if m = 0, these fields are omitted).		
	The above 5 fields are repeated k – 1 times.		

17.2.5 Associated Clients TLV format

Table 15 provides the definition for the Associated Clients TLV.

Table 15. Associated Clients TLV format

Field	Length	Value	Description
tlvType	1 octet	0x84	Associated Clients TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	k	Number of BSSs included in this TLV.
	6 octets	Any EUI-48 value	The BSSID of the BSS operated by the Multi-AP Agent in which the client is associated.
	2 octets	m	Number of clients associated to the BSS.
	6 octets	Any EUI-48 value	The MAC address of the associated 802.11 client.
	2 octets	0x0000 – 0xFFFE: 0 - 65,534 0xFFFF: 65,535 or higher	Time since the 802.11 client's last association to this Multi-AP device in seconds.
	The above 2 fields are repeated m – 1 times (if m = 0, these fields are omitted).		
	The above 4 fields are repeated k – 1 times.		

17.2.6 AP Capability TLV format

Table 16 provides the definition for the AP Capability TLV.

Table 16. AP Capability TLV format

Field	Length	Value	Description
tlvType	1 octet	0xA1	AP Capability TLV.
tlvLength	2 octets	1	Number of octets in ensuing field.
tlvValue	bit 7	0: Not supported 1: Supported	Support Unassociated STA Link Metrics reporting on the channels its BSSs are currently operating on.
	bit 6	0: Not supported 1: Supported	Support Unassociated STA Link Metrics reporting on channels its BSSs are not currently operating on.

Field	Length	Value	Description
	bit 5	0: Not supported 1: Supported	Support Agent-initiated RCPI-based Steering.
	bits 4-0		Reserved

17.2.7 AP Radio Basic Capabilities TLV format

Table 17 provides the definition for the AP Radio Basic Capabilities TLV.

Table 17. AP Radio Basic Capabilities TLV format

Field	Length	Value	Description
tlvType	1 octet	0x85	AP Radio Basic Capabilities TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio unique identifier of the radio for which capabilities are reported.
	1 octet	Variable (non-zero)	Maximum number of BSSs supported by this radio.
	1 octet	k	Number of operating classes supported for the radio, defined per Table E-4 in [1]. All the supported operating classes are reported per regulatory restrictions.
	1 octet	Variable	Operating class per Table E-4 in [1], that this radio is capable of operating on.
	1 octet	Variable	Maximum transmit power EIRP that this radio is capable of transmitting in the current regulatory domain for the operating class. The field is coded as a 2's complement signed integer in units of decibels relative to 1 mW (dBm).
	1 octet	m	Number of statically Non-operable channels in the operating class. Other channels from this operating class which are not listed here are supported for the radio.
	1 octet	Variable	Channel number of a channel which is statically a Non-operable channel in the operating class (i.e. the radio is never able to operate on this channel). This field is not present if $m = 0$.
	The above field is repeated $m - 1$ times (if $m = 0$, these fields are omitted).		
	The above 4 fields are repeated $k - 1$ times.		

17.2.8 AP HT Capabilities TLV format

Table 18 provides the definition for the AP HT Capabilities TLV.

Table 18. AP HT Capabilities TLV format

Field	Length	Value	Description
tlvType	1 octet	0x86	AP HT Capabilities TLV.
tlvLength	2 octets	7	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	Radio unique identifier of the radio for which HT capabilities are reported.

Field	Length	Value	Description
	bits 7-6	00: 1 Tx spatial stream 01: 2 Tx spatial stream 10: 3 Tx spatial stream 11: 4 Tx spatial stream	Maximum number of supported Tx spatial streams.
	bits 5-4	00: 1 Rx spatial stream 01: 2 Rx spatial stream 10: 3 Rx spatial stream 11: 4 Rx spatial stream	Maximum number of supported Rx spatial streams.
	bit 3	0: Not supported 1: Supported	Short GI Support for 20 MHz.
	bit 2	0: Not supported 1: Supported	Short GI Support for 40 MHz.
	bit 1	0: Not supported 1: Supported	HT support for 40 MHz.
	bit 0		Reserved.

17.2.9 AP VHT Capabilities TLV format

Table 19 provides the definition for the AP VHT Capabilities TLV.

Table 19. AP VHT Capabilities TLV format

Field	Length	Value	Description
tlvType	1 octet	0x87	AP VHT Capabilities TLV.
tlvLength	2 octets	12	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	Radio unique identifier of the radio for which VHT capabilities are reported.
	2 octets	Variable	Supported VHT Tx MCS. Supported set of VHT MCSs that can be transmitted. Set to Tx VHT MCS Map field per Figure 9-562 in [1] reordered from the underlying referenced standard into big-endian order.
	2 octets	Variable	Supported VHT Rx MCS. Supported set of VHT MCSs that can be received. Set to Rx VHT MCS Map field per Figure 9-562 in [1] reordered from the underlying referenced standard into big-endian order.
	bits 7-5	000: 1 Tx spatial stream 001: 2 Tx spatial stream 010: 3 Tx spatial stream 011: 4 Tx spatial stream 100: 5 Tx spatial stream 101: 6 Tx spatial stream 110: 7 Tx spatial stream 111: 8 Tx spatial stream	Maximum number of supported Tx spatial streams.

Field	Length	Value	Description
	bits 4-2	000: 1 Rx spatial stream 001: 2 Rx spatial stream 010: 3 Rx spatial stream 011: 4 Rx spatial stream 100: 5 Rx spatial stream 101: 6 Rx spatial stream 110: 7 Rx spatial stream 111: 8 Rx spatial stream	Maximum number of supported Rx spatial streams.
	bit 1	0: Not supported 1: Supported	Short GI support for 80 MHz.
	bit 0	0: Not supported 1: Supported	Short GI support for 160 MHz and 80+80 MHz.
	bit 7	0: Not supported 1: Supported	VHT support for 80+80 MHz.
	bit 6	0: Not supported 1: Supported	VHT support for 160 MHz.
	bit 5	0: Not supported 1: Supported	SU beamformer capable.
	bit 4	0: Not supported 1: Supported	MU beamformer capable.
	bits 3-0		Reserved.

17.2.10 AP HE Capabilities TLV format

Table 20 provides the definition for the AP HE Capabilities TLV.

Table 20. AP HE Capabilities TLV format

Field	Length	Value	Description
tlvType	1 octet	0x88	AP HE Capabilities TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	Radio unique identifier of the radio for which HE capabilities are reported.
	1 octet	k	Length of supported HE MCS field.
	k octets	Variable	Supported HE MCS indicating set of supported HE Tx and Rx MCS. Set to Tx Rx HE MCS Support field from 802.11ax spec reordered from the underlying referenced standard into big-endian order. Variable length from 2-12 bytes.
	bits 7-5	000: 1 Tx spatial stream 001: 2 Tx spatial stream 010: 3 Tx spatial stream 011: 4 Tx spatial stream 100: 5 Tx spatial stream 101: 6 Tx spatial stream 110: 7 Tx spatial stream 111: 8 Tx spatial stream	Maximum number of supported Tx spatial streams.

Field	Length	Value	Description
	bits 4-2	000: 1 Rx spatial stream 001: 2 Rx spatial stream 010: 3 Rx spatial stream 011: 4 Rx spatial stream 100: 5 Rx spatial stream 101: 6 Rx spatial stream 110: 7 Rx spatial stream 111: 8 Rx spatial stream	Maximum number of supported Rx spatial streams.
	bit 1	0: Not supported 1: Supported	HE support for 80+80 MHz.
	bit 0	0: Not supported 1: Supported	HE support for 160 MHz.
	bit 7	0: Not supported 1: Supported	SU beamformer capable.
	bit 6	0: Not supported 1: Supported	MU beamformer capable.
	bit 5	0: Not supported 1: Supported	UL MU-MIMO capable.
	bit 4	0: Not supported 1: Supported	UL MU-MIMO + OFDMA capable.
	bit 3	0: Not supported 1: Supported	DL MU-MIMO + OFDMA capable.
	bit 2	0: Not supported 1: Supported	UL OFDMA capable.
	bit 1	0: Not supported 1: Supported	DL OFDMA capable.
	bit 0		Reserved.

17.2.11 Steering Policy TLV format

Table 21 provides the definition for the Steering Policy TLV.

Table 21. Steering Policy TLV format

Field	Length	Value	Description
tlvType	1 octet	0x89	Steering Policy TLV.
tlvLength	2 octets	variable	Number of octets in ensuing field.
tlvValue	1 octet	h	Local Steering Disallowed STA count Number of STA MAC addresses for which local steering is disallowed.
	6 octets	Any EUI-48 value	STA MAC address for which local steering is disallowed. Not included if previous field is set to zero.
	The above field is repeated h – 1 times.		
	1 octet	k	BTM Steering Disallowed STA count. Number of STA MAC addresses for which BTM steering is disallowed.
	6 octets	Any EUI-48 value	STA MAC address for which BTM steering is disallowed. Not included if previous field is set to zero.

Field	Length	Value	Description
The above field is repeated $k - 1$ times.			
	1 octet	m	Number of radios for which control policy is being indicated.
	6 octets	Any EUI-48 value	Radio unique identifier of an AP radio for which Multi-AP control policies are being provided.
	1 octet	0x00: Agent Initiated Steering Disallowed 0x01: Agent Initiated RCPI-based Steering Mandated 0x02: Agent Initiated RCPI-based Steering Allowed 0x03 – 0xFF: Reserved	Steering Policy.
	1 octet	variable	Channel Utilization Threshold (defined per BSS Load element section 9.4.2.28 of [1]).
	1 octet	Variable 0 – 220: RCPI threshold (encoded per Table 9-154 of [1]). 221 – 255: Reserved	RCPI Steering Threshold.
The above 4 fields are repeated for $m - 1$ times.			

17.2.12 Metric Reporting Policy TLV format

Table 22 provides the definition for the Metric Reporting Policy TLV.

Table 22. Metric Reporting Policy TLV format

Field	Length	Value	Description
tlvType	1 octet	0x8A	Metric Reporting Policy TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	Variable 0: Do not report AP Metrics periodically 1 – 255: AP Metrics reporting interval in seconds	AP Metrics Reporting Interval in seconds.
	1 octet	k	Number of radios.
	6 octets	Variable	Radio Unique Identifier.
	1 octet	Variable 0: Do not report STA Metrics based on RCPI threshold. 1 – 220: RCPI threshold (encoded per Table 9-154 of [1]). 221 – 255: Reserved.	STA Metrics Reporting RCPI Threshold.
	1 octet	0: Use Agent's implementation-specific default RCPI Hysteresis margin. >0: RCPI hysteresis margin value	STA Metrics Reporting RCPI Hysteresis Margin Override. This field is coded as an unsigned integer in units of decibels (dB). Note: Setting this field to a non-zero value may cause suboptimal performance.

Field	Length	Value	Description
	1 octet	Unsigned integer 0: Do not report AP Metrics based on Channel utilization threshold. >0: AP Metrics Channel Utilization Reporting Threshold (similar to channel utilization measurement in 9.4.2.28 of [1]).	AP Metrics Channel Utilization Reporting Threshold.
	bit 7	0: Do not include Associated STA Traffic Stats TLV in AP Metrics Response 1: Include Associated STA Traffic Stats TLV in AP Metrics Response	Associated STA Traffic Stats Inclusion Policy. Note: Inclusion of STA Traffic Stats TLV(s) in STA Metrics Response messages may significantly impact the throughput performance of the corresponding radio.
	bit 6	0: Do not include Associated STA Link Metrics TLV in AP Metrics Response 1: Include Associated STA Link Metrics TLV in AP Metrics Response	Associated STA Link Metrics Inclusion Policy.
	bits 5-0		Reserved.
The above 7 fields are repeated k – 1 times.			

17.2.13 Channel Preference TLV format

Table 23 provides the definition for the Channel Preference TLV.

Table 23. Channel Preference TLV format

Field	Length	Value	Description
tlvType	1 octet	0x8B	Channel Preference TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique identifier of a radio for which channel preferences are reported.
	1 octet	m	Number of operating classes for which preferences are reported in this TLV.
	1 octet	Variable	Operating Class contains an enumerated value from Table E-4 in Annex E of [1], specifying the global operating class in which the subsequent Channel List is valid.
	1 octet	k	Number of channels specified in the Channel List.
	k octets	Variable	Channel List. Contains a variable number of octets. Each octet describes a single channel number in the Operating Class. An empty Channel List field (k=0) indicates that the indicated Preference applies to all channels in the Operating Class.

Field	Length	Value	Description
	bits 7-4	0000: Non-operable channel 0001-1110: Operable with preference score 1 - 14 (where 1 is least preferred) 1111: Reserved Note: the “most preferred” score 15 is inferred for all channels / operating classes that are not specified in the corresponding message.	Preference. Indicates a preference value for the channels in the Channel List.
	bits 3-0	0000: Unspecified 0001: Proximate non-802.11 interferer in local environment 0010: Intra-network 802.11 OBSS interference management 0011: External network 802.11 OBSS interference management 0100: Reduced coverage (e.g. due to limited transmit power) 0101: Reduced throughput (e.g. due to limited channel bandwidth of the operating class, or high channel utilization measured on the channel) 0110: In-device Interferer within AP (can only be specified by the Multi-AP Agent) 0111: Operation disallowed due to radar detection on a DFS channel (can only be specified by the Multi-AP Agent) 1000: Operation would prevent backhaul operation using shared radio (can only be specified by the Multi-AP Agent) 1001: Immediate operation possible on a DFS channel – CAC has been run and is still valid and channel has been cleared for use (can only be specified by the Multi-AP Agent) 1010: DFS channel state unknown (CAC has not run or its validity period has expired) (can only be specified by the Multi-AP Agent) 1011: Controller DFS Channel Clear Indication (Can only be specified by the Multi-AP Controller) 1100 – 1111: Reserved	Reason Code. Indicates the reason for the Preference.
The above 5 fields are repeated m – 1 times.			

17.2.14 Radio Operation Restriction TLV format

Table 24 provides the definition for the Radio Operation Restriction TLV.

Table 24. Radio Operation Restriction TLV format

Field	Length	Value	Description
tlvType	1 octet	0x8C	Radio Operation Restriction TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique identifier of a radio.
	1 octet	m	Number of Operating Classes for which restrictions are reported in this TLV.
	1 octet	Variable	Operating Class contains an enumerated value from Table E-4 in Annex E of [1], specifying the global operating class in which the subsequent Channel List is valid.

Field	Length	Value	Description
	1 octet	k	Number of channels specified.
	1 octet	Variable	Channel number for which a restriction applies.
	1 octet	0x00 – 0xFF	The minimum frequency separation (in multiples of 10 MHz) that this radio would require when operating on the above channel number between the center frequency of that channel and the center operating frequency of another radio (operating simultaneous TX/RX) of the Multi-AP Agent.
	The above 2 fields are repeated k – 1 times		
	The above 4 fields are repeated m – 1 times		

17.2.15 Transmit Power Limit TLV format

Table 25 provides the definition for the Transmit Power Limit TLV.

Table 25. Transmit Power Limit TLV format

Field	Length	Value	Description
tlvType	1 octet	0x8D	Transmit Power TLV.
tlvLength	2 octets	7	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique identifier.
	1 octet	Variable	Transmit Power Limit EIRP per 20 MHz bandwidth representing the nominal transmit power limit for this radio. The field is coded as a 2's complement signed integer in units of decibels relative to 1 mW (dBm).

17.2.16 Channel Selection Response TLV format

Table 26 provides the definition for the Channel Selection Response TLV.

Table 26. Channel Selection Response TLV format

Field	Length	Value	Description
tlvType	1 octet	0x8E	Channel Selection Response TLV.
tlvLength	2 octets	7	Number of octets in ensuing field.
tlvValue	6 octets		Radio unique identifier.
	1 octet	0x00: Accept 0x01: Decline because request violates current preferences which have changed since last reported 0x02: Decline because request violates most recently reported preferences 0x03: Decline because request would prevent operation of a currently operating backhaul link (where backhaul STA and BSS share a radio) 0x04 – 0xFF: Reserved	Indicates the channel selection response code, with respect to the Channel Selection Request.

17.2.17 Operating Channel Report TLV format

Table 27 provides the definition for the Operating Channel Report TLV.

Table 27. Operating Channel Report TLV format

Field	Length	Value	Description
tlvType	1 octet	0x8F	Operating Channel TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique identifier of a radio.
	1 octet	k	Number of current operating classes.
	1 octet	Variable	Operating Class. It contains an enumerated value from Table E-4 in Annex E of [1], specifying the global operating class in which the subsequent Channel is valid.
	1 octet	Variable	Current operating channel number in the Operating Class.
	The above 2 fields are repeated k – 1 times.		
	1 octet	Variable	Current Transmit Power EIRP representing the current nominal transmit power. The field is coded as a 2's complement signed integer in units of decibels relative to 1 mW (dBm). This value is less than or equal to the Maximum Transmit Power specified in the AP Radio Basic Capabilities TLV for the current operating class.

17.2.18 Client Info TLV format

Table 28 provides the definition for the Client Info TLV.

Table 28. Client Info TLV format

Field	Length	Value	Description
tlvType	1 octet	0x90	Client info TLV.
tlvLength	2 octets	12	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	The BSSID of a BSS.
	6 octets	Any EUI-48 value	The MAC address of the client.

17.2.19 Client Capability Report TLV format

Table 29 provides the definition for the Client Capability Report TLV.

Table 29. Client Capability Report TLV format

Field	Length	Value	Description
tlvType	1 octet	0x91	Client capability report TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	0x00: Success 0x01: Failure 0x02 – 0xFF: Reserved	Result Code for the client capability report message.

Field	Length	Value	Description
	Variable		The frame body of the most recently received (Re)Association Request frame from this client, as defined in Table 9-29 and Table 9-31 of [1] in the order of the underlying referenced standard. If Result Code is not equal to 0x00, this field is omitted.

17.2.20 Client Association Event TLV format

Table 30 provides the definition for the Client Association Event TLV.

Table 30. Client Association Event TLV format

Field	Length	Value	Description
tlvType	1 octet	0x92	Client Association Event TLV.
tlvLength	2 octets	13	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	The MAC address of the client.
	6 octets	Any EUI-48 value	The BSSID of the BSS operated by the Multi-AP Agent for which the event has occurred.
	bit 7	1: Client has joined the BSS 0: Client has left the BSS	Association event.
	bits 6-0	0	Reserved.

17.2.21 AP Metric Query TLV format

Table 31 provides the definition for the AP metrics query TLV.

Table 31. AP Metric Query TLV format

Field	Length	Value	Description
tlvType	1 octet	0x93	AP metrics query TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	k	Number of BSSIDs included in this TLV
	6 octets	Any EUI-48 value	BSSID of a BSS operated by the Multi-AP device for which the metrics are to be reported.
	The above field is repeated k – 1 times.		

17.2.22 AP Metrics TLV format

Table 32 provides the definition for the AP Metrics TLV.

Table 32. AP Metrics TLV format

Field	Length	Value	Description
tlvType	1 octet	0x94	AP metrics TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	BSSID of a BSS operated by the Multi-AP Agent for which the metrics are reported.
	1 octet	Variable	Channel Utilization as measured by the radio operating the BSS as defined in BSS Load element section 9.4.2.28 of [1].

Field	Length	Value	Description
	2 octets	Variable	Unsigned integer indicating the total number of STAs currently associated with this BSS.
	bit 7	1	Include bit for the Estimated Service Parameters Information field for AC=BE. This field shall be set to 1.
	bit 6	0 or 1	Include bit for the Estimated Service Parameters Information field for AC=BK.
	bit 5	0 or 1	Include bit for the Estimated Service Parameters Information field for AC=VO.
	bit 4	0 or 1	Include bit for the Estimated Service Parameters Information field for AC=VI.
	bits 3 - 0	0	Reserved.
	3 octets	Variable	Estimated Service Parameters Information field for AC=BE (see Figure 9-588 in [1]), containing Data Format, BA Window Size, Estimated Air Time Fraction and Data PPDU Target Duration subfields reordered from the underlying referenced standard into big-endian order.
	0 or 3 octets	Variable	If bit 6 of the 10th octet of tlvValue is set to 1, this field shall be included. Otherwise, this field shall be omitted. Estimated Service Parameters Information field for AC=BK (see Figure 9-588 in [1]), containing Data Format, BA Window Size, Estimated Air Time Fraction and Data PPDU Target Duration subfields reordered from the underlying referenced standard into big-endian order.
	0 or 3 octets	Variable	If bit 5 of the 10th octet of tlvValue is set to 1, this field shall be included. Otherwise, this field shall be omitted. Estimated Service Parameters Information field for AC=VO (see Figure 9-588 in [1]), containing Data Format, BA Window Size, Estimated Air Time Fraction and Data PPDU Target Duration subfields reordered from the underlying referenced standard into big-endian order.
	0 or 3 octets	Variable	If bit 4 of the 10th octet of tlvValue is set to 1, this field shall be included. Otherwise, this field shall be omitted. Estimated Service Parameters Information field for AC=VI (see Figure 9-588 in [1]), containing Data Format, BA Window Size, Estimated Air Time Fraction and Data PPDU Target Duration subfields reordered from the underlying referenced standard into big-endian order.

17.2.23 STA MAC Address Type TLV format

Table 33 provides the definition for the STA MAC Address Type TLV.

Table 33. STA MAC Address Type TLV format

Field	Length	Value	Description
tlvType	1 octet	0x95	STA MAC address TLV.
tlvLength	2 octets	6	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	MAC address of the associated STA.

17.2.24 Associated STA Link Metrics TLV format

Table 34 provides the definition for the Associated STA Link Metrics TLV.

Table 34. Associated STA Link Metrics TLV format

Field	Length	Value	Description
tlvType	1 octet	0x96	Associated STA link metrics TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	MAC address of the associated STA.
	1 octet	k (≥ 0)	Number of BSSIDs reported for this STA.
	6 octets	Any EUI-48 value	BSSID of the BSS for which the STA is associated.
	4 octets	Variable	The time delta in ms between the time at which the earliest measurement that contributed to the data rate estimates were made, and the time at which this report was sent.
	4 octets	Variable	Estimated MAC Data Rate in downlink (in Mb/s).
	4 octets	Variable	Estimated MAC Data Rate in uplink (in Mb/s).
	1 octet	Variable 0 – 220: RCPI (encoded per Table 9-154 of [1]). 221 - 255: Reserved.	Uplink RCPI for STA.
	The above 5 fields are repeated k – 1 times (if k = 0, these fields are omitted).		

17.2.25 Unassociated STA Link Metrics Query TLV format

Table 35 provides the definition for the Unassociated STA Link Metrics Query TLV.

Table 35. Unassociated STA Link Metrics Query TLV format

Field	Length	Value	Description
tlvType	1 octet	0x97	Unassociated STA link metrics query TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	Variable	Operating Class contains an enumerated value from table E-4 in Annex E of [1], specifying the global operating class in which the Channel List is valid.
	1 octet	k	Number of channels specified in the Channel List.
	1 octet	Variable	Channel Number. A channel number in the Operating Class on which the RCPI measurements are to be made. Channel numbering dependent on Operating Class according to Annex E of [1].
	1 octet	m	Number of STA MAC addresses for this channel.
	6 octets	Any EUI-48 value	STA MAC address for which the metrics are requested.
	The above field is repeated m – 1 times.		
	The above three fields are repeated k – 1 times.		

17.2.26 Unassociated STA Link Metrics Response TLV format

Table 36 provides the definition for the Unassociated STA Link Metrics Response TLV.

Table 36. Unassociated STA Link Metrics Response TLV format

Field	Length	Value	Description
tlvType	1 octet	0x98	Unassociated STA link metrics response TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	Variable	Operating Class contains an enumerated value from table E-4 in Annex E of [1], specifying the global operating class for which the Channels in the report apply.
	1 octet	k (>=0)	The number of STA entries included in this TLV.
	6 octets	Any EUI-48 value	MAC address of STA for which UL RCPI is being reported.
	1 octet	Variable	A single channel number in Operating Class on which the RCPI measurement for STA was made. Channel numbering is dependent on Operating Class according to Annex E of [1].
	4 octets	Variable	The time delta in ms between the time at which the RCPI for STA was measured, and the time at which this report was sent.
	1 octet	Variable 0 – 220: RCPI (encoded per Table 9-154 of [1]). 221 - 255: Reserved.	Uplink RCPI for STA.
	The above 4 fields are repeated k – 1 times (if k = 0, these fields are omitted).		

17.2.27 Beacon Metrics Query TLV format

Table 37 provides the definition for the Beacon Metrics Query TLV.

Table 37. Beacon Metrics Query TLV format

Field	Length	Value	Description
tlvType	1 octet	0x99	Beacon Metrics Query TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	MAC address of the associated STA for which the Beacon report information is requested.
	1 octet	Variable	Operating Class field to be specified in the Beacon request.
	1 octet	Variable	Channel Number field to be specified in the Beacon request.
	6 octets	Variable	BSSID field to be specified in the Beacon request.
	1 octet	Variable	Reporting Detail value to be specified in the Beacon request.
	1 octet	g	SSID length.
	g octets	Variable	SSID
	1 octet	h	Number of AP Channel Reports. If the value of Channel Number field is not set to 255, h is set to 0.
	1 octet	k	Length of an AP Channel Report.
	1 octet	Variable	Operating Class in an AP Channel Report.
	k – 1 octets	Variable	Channel List in an AP Channel Report.
	The above 3 fields are repeated h – 1 times (if h = 0, these fields are omitted).		

Field	Length	Value	Description
	1 octet	m	Number of element IDs. If the value of Reporting Detail field is not set to 1, m is set to 0.
	m octets	Variable	Element List. Comprises a list of m Element IDs to be included in a Request Element in the Beacon request.

17.2.28 Beacon Metrics Response TLV format

Table 38 provides the definition for the Beacon Metrics Response TLV.

Table 38. Beacon Metrics Response TLV format

Field	Length	Value	Description
tlvType	1 octet	0x9A	Beacon metrics response TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	MAC address of the associated STA for which the Beacon Report information is requested.
	1 octet		Reserved.
	1 octet	k	Number of measurement report elements included in this TLV.
	Variable	Variable	Contains a Measurement Report element that was received from the STA since the corresponding Beacon Metrics Query message was received by the Multi-AP Agent, per Figure 9-199 in [1] in the order of the underlying referenced standard. The length of this field is carried in the 2nd octet of the element per Figure 9-122 in [1].
	The above field is repeated k - 1 times.		

17.2.29 Steering Request TLV format

Table 39 provides the definition for the Steering Request TLV.

Table 39. Steering Request TLV format

Field	Length	Value	Description
tlvType	1 octet	0x9B	Steering Request TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	BSSID. Unique identifier of the source BSS for which the steering request applies (i.e. BSS that the STAs specified in the request are currently associated with).
	bit 7	0: Request is a Steering Opportunity. 1: Request is a Steering Mandate to trigger steering for specific client STA(s)	Request Mode.
	bit 6	Variable	BTM Disassociation Imminent bit.
	bit 5	Variable	BTM Abridged bit.
	bits 4-00	0	Reserved.

Field	Length	Value	Description
	2 octets	Variable	Steering Opportunity window. Time period in seconds (from reception of the Steering Request message) for which the request is valid. If Request Mode bit is 1, then the value of this field is ignored.
	2 octets	Variable	BTM Disassociation Timer. Time period in TUs of the disassociation timer in the BTM Request.
	1 octet	k = 0: Steering request applies to all associated STAs in the BSS per policy setting. k > 0: Steering request applies to specific STAs specified by STA MAC address(es)	STA List Count k.
	6 octets	Variable	STA MAC address for which the steering request applies. If k is 0, then this field is not included.
The above field is repeated k – 1 times (if k = 0, this field is omitted).			
	1 octet	m = 1 or k	Target BSSID List Count. If Request Mode bit is set to 1 and if: m = 1: The same target BSSID is indicated for all specified STAs m = k (k>1): An individual target BSSID is indicated for each specified STA (in the same order) If Request Mode bit is 0, then this field is set to zero.
	6 octets	Variable	Target BSSID. Indicates a target BSSID for steering. Wildcard BSSID is represented by FF:FF:FF:FF:FF:FF.
	1 octet	Variable	Target BSS Operating Class. If the Target BSSID is set to "Wildcard BSSID", the value of this field is ignored by the receiver.
	1 octet	Variable	Target BSS Channel Number for channel on which the Target BSS is transmitting Beacon frames. If the Target BSSID is set to "Wildcard BSSID", the value of this field is ignored by the receiver.
The above 3 fields are repeated m – 1 times (if m = 0, these fields are omitted).			

17.2.30 Steering BTM Report TLV format

Table 40 provides the definition for the Steering BTM Report TLV.

Table 40. Steering BTM Report TLV format

Field	Length	Value	Description
tlvType	1 octet	0x9C	Steering BTM Report TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	BSSID. Unique identifier of the source BSS for which the steering BTM report applies.
	6 octets	Variable	STA MAC address for which the steering BTM report applies.

Field	Length	Value	Description
	1 octet	Variable	BTM Status Code. Indicates the value of the BTM Status Code as reported by the STA in the BTM Response (per Table 9-357 in [1]).
	0 or 6 octets	Variable	Target BSSID. Indicates the value of the Target BSSID field (if present) in the BTM Response received from the STA (see 9.6.14.10 of [1]). Note: This indicates the BSSID that the STA intends to roam to, which may not align with the Target BSSID specified in the BTM Request.

17.2.31 Client Association Control Request TLV format

Table 41 provides the definition for the Client Association Control Request TLV.

Table 41. Client Association Control Request TLV format

Field	Length	Value	Description
tlvType	1 octet	0x9D	Client Association Control Request TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	BSSID - unique identifier of the BSS for which the client blocking request applies.
	1 octet	0x00: Block 0x01: Unblock 0x02-0xFF: Reserved	Association Control. Indicates if the request is to block or unblock the indicated STAs from associating.
	2 octets	Variable	Validity Period. Time period in seconds (from reception of the Client Association Control Request message) for which a blocking request is valid.
	1 octet	k	STA List Count Indicating one or more STA(s) for which Client Association Control request applies.
	6 octets	Variable	STA MAC address for which the Client Association Control request applies.
	The above field is repeated k – 1 times.		

17.2.32 Backhaul Steering Request TLV format

Table 42 provides the definition for the Backhaul Steering Request TLV.

Table 42. Backhaul Steering Request TLV format

Field	Length	Value	Description
tlvType	1 octet	0x9E	Backhaul Steering Request TLV.
tlvLength	2 octets	14	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	The MAC address of the associated backhaul STA operated by the Multi-AP Agent.
	6 octets	Any EUI-48 value	The BSSID of the target BSS.
	1 octet	Variable	Operating class per Table E-4 in [1].
	1 octet	Variable	Channel number on which Beacon frames are being transmitted by the target BSS.

17.2.33 Backhaul Steering Response TLV format

Table 43 provides the definition for the Backhaul Steering Response TLV.

Table 43. Backhaul Steering Response TLV format

Field	Length	Value	Description
tlvType	1 octet	0x9F	Backhaul steering response TLV.
tlvLength	2 octets	13	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	The MAC address of the associated backhaul STA operated by the Multi-AP Agent.
	6 octets	Any EUI-48 value	The BSSID of the target BSS.
	1 octet	0x00: Success 0x01: Failure 0x02 – 0xFF: Reserved.	Result code.

17.2.34 Higher Layer Data TLV format

Table 44 provides the definition for the Higher Layer Data TLV.

Table 44. Higher Layer Data TLV format

Field	Length	Value	Description
tlvType	1 octet	0xA0	Higher layer data TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	Variable	Higher layer protocol (see Appendix A.1).
	Variable	Variable	Higher layer protocol payload (To be defined for specific higher layer protocol).

17.2.35 Associated STA Traffic Stats TLV format

Table 45 provides the definition for the Associated STA Traffic Stats TLV.

Table 45. Associated STA Traffic Stats TLV

Field	Length	Value	Description
tlvType	1 octet	0xA2	Associated STA Traffic Stats TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	MAC address of the associated STA.
	4 octets	Unsigned Integer	BytesSent Raw counter of the number of bytes sent to the associated STA. Note: it is the responsibility of the recipient to handle counter roll-over. For Multi-AP Agents that implement Profile-1, the units of this counter are Bytes. Otherwise, the units of this counter are as specified by the Byte Counter Units field of the Profile-2 AP Capability TLV.

Field	Length	Value	Description
	4 octets	Unsigned Integer	BytesReceived Raw counter of number of bytes received from the associated STA. Note: it is the responsibility of the recipient to handle counter roll-over. For Multi-AP Agents that implement Profile-1, the units of this counter are Bytes. Otherwise, the units of this counter are as specified by the Byte Counter Units field of the Profile-2 AP Capability TLV.
	4 octets	Unsigned Integer	PacketsSent Raw counter of the number of packets successfully sent to the associated STA. Note: it is the responsibility of the recipient to handle counter roll-over.
	4 octets	Unsigned Integer	PacketsReceived Raw counter of the number of packets received from the associated STA during the measurement window. Note: it is the responsibility of the recipient to handle counter roll-over.
	4 octets	Unsigned Integer	TxPacketsErrors Raw counter of the number of packets which could not be transmitted to the associated STA due to errors. Note: it is the responsibility of the recipient to handle counter roll-over.
	4 octets	Unsigned Integer	RxPacketsErrors Raw counter of the number of packets which were received in error from the associated STA. Note: it is the responsibility of the recipient to handle counter roll-over.
	4 octets	Unsigned Integer	RetransmissionCount Raw counter of the number of packets sent with the retry flag set to the associated STA. Note: it is the responsibility of the recipient to handle counter roll-over.

17.2.36 Error Code TLV format

Table 46 provides the definition for the Error Code TLV.

Table 46. Error Code TLV format

Field	Length	Value	Description
tlvType	1 octet	0xA3	Error code TLV.
tlvLength	2 octets	7	Number of octets in ensuing field.

Field	Length	Value	Description
tlvValue	1 octet	0x00: Reserved 0x01: STA associated with a BSS operated by the Multi-AP Agent. 0x02: STA not associated with any BSS operated by the Multi-AP Agent. 0x03: Client capability report unspecified failure 0x04: Backhaul steering request rejected because the backhaul STA cannot operate on the channel specified. 0x05: Backhaul steering request rejected because the target BSS signal is too weak or not found. 0x06: Backhaul steering request authentication or association Rejected by the target BSS. 0x07 – 0xFF: Reserved.	Reason code.
	6 octets	Any EUI-48 value	The MAC address of the STA referred to in the previous field. The value of this field is valid only if the reason code field is set to 0x01 or 0x02. Otherwise this field is ignored by the recipient of this TLV.

17.2.37 Channel Scan Reporting Policy TLV format

Table 47 provides the definition for the Channel Scan Reporting Policy TLV.

Table 47. Channel Scan Reporting Policy TLV

Field	Length	Value	Description
tlvType	1 octet	0xA4	Channel Scan Reporting Policy TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	bit 7	1: Report Independent Channel Scans 0: Do not report Independent Channel Scans unless explicitly requested in a Channel Scan Request	Report Independent Channel Scans
	bits 6-0		Reserved

17.2.38 Channel Scan Capabilities TLV format

Table 48 provides the definition for the Channel Scan Capabilities TLV.

Table 48. Channel Scan Capabilities TLV

Field	Length	Value	Description
tlvType	1 octet	0xA5	Channel Scan Capabilities TLV.
tlvLength	2 octets	Variable	Number of Octets in ensuing field.
tlvValue	1 octet	R	Number of Radios The number of radios for which channel scan capabilities are declared.
	6 octets	Variable	Radio Unique Identifier of a radio of the Multi-AP Agent.
	bit 7	1: True (Agent can only perform scan on boot) 0: False (Agent can perform Requested scans)	On Boot Only Indicates whether the specified radio is capable only of “On boot” scans or can perform scans upon request.
	bits 6-5	0x00: No impact (independent radio is available for scanning that is not used for Fronthaul or backhaul) 0x01: Reduced number of spatial streams 0x02: Time slicing impairment (Radio may go off channel for a series of short intervals) 0x03: Radio unavailable for >= 2 seconds)	Scan Impact Guidance information on the expected impact on any Fronthaul or Backhaul operations on this radio of using this radio to perform a channel scan.
	bits 4-0		Reserved
	4 octets	Variable	Minimum Scan Interval The minimum interval in seconds between the start of two consecutive channel scans on this radio
	1 octet	m	Number of Operating Classes Number of operating classes for which channel scan capabilities are declared on this radio.
	1 octet	Variable	Operating Class Operating Class contains an enumerated value from Table E-4 in Annex E of [1].
	1 octet	k	Number of Channels. Number of channels specified in the Channel List. k=0 indicates that the Multi-AP Agent is capable of scanning on all channels in the Operating Class.
	k octets	Variable	Channel List. Contains a variable number of octets. Each octet describes a single channel number in the Operating Class on which the Multi-AP Agent is capable of performing a scan. If k=0, this field is omitted.
	The above 3 fields are repeated m – 1 times.		
	The above 9 fields are repeated r -1 times.		

17.2.39 Channel Scan Request TLV format

Table 49 provides the definition for the Channel Scan Request TLV.

Table 49. Channel Scan Request TLV

Field	Length	Value	Description
tlvType	1 octet	0xA6	Channel Scan Request TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	bit 7	1: Perform a fresh scan and return results 0: Return stored results of last successful scan	Perform Fresh Scan Indicator to identify whether a fresh scan is being requested, or whether stored results from previous (including on-boot) scan are requested.
	bits 6-0		Reserved
	1 octet	r	Number of Radios The number of radios upon which channel scans are requested.
	6 octets	Variable	Radio Unique Identifier of a radio of the Multi-AP Agent.
	1 octet	m	Number of Operating Classes Number of operating classes for which channel scans are being requested on this radio. If the Perform Fresh Scan bit is set to 0, this field shall be set to zero and the following fields shall be omitted.
	1 octet	Variable	Operating Class Operating Class contains an enumerated value from Table E-4 in Annex E of [1], specifying the global operating class in which the subsequent Channel List is valid.
	1 octet	k	Number of Channels. Number of channels specified in the Channel List. k=0 indicates that the Multi-AP Agent is requested to scan on all channels in the Operating Class.
	k octets	Variable	Channel List. Contains a variable number of octets. Each octet describes a single channel number in the Operating Class on which the Multi-AP Agent is requested to perform a scan. If k=0, this field is omitted.
	The above 3 fields are present m times.		
	The above 5 fields are repeated r - 1 times.		

17.2.40 Channel Scan Result TLV format

Table 50 provides the definition for the Channel Scan Result TLV.

Table 50. Channel Scan Result TLV

Field	Length	Value	Description
tlvType	1 octet	0xA7	Channel Scan Result TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique Identifier of a radio of the Multi-AP Agent.
	1 octet	Variable	Operating Class
	1 octet	Variable	Channel The channel number of the channel scanned by the radio given the operating class.

Field	Length	Value	Description
	1 octet	0x00: Success 0x01: Scan not supported on this operating class and channel on this radio 0x02: Request too soon after last scan 0x03: Radio too busy to perform scan 0x04: Scan not completed 0x05: Scan aborted 0x06: Fresh scan not supported. Radio only supports on boot scans. 0x07 – 0xFF: Reserved.	Scan Status A status code to indicate whether a scan has been performed successfully and if not, the reason for failure.
	The following fields are only present if Scan Status is set to 0x00		
	1 octet	Variable	Timestamp Length
	Timestamp Length Octets	Variable	TimeStamp The start time of the scan of the channel. The timestamp shall be formatted as a string using the typedef date-and-time string format as defined in section 3 of [1] and shall include time-sefrac and time-offset as defined in section 5.6 of [1]. '\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}\.\d+Z [\+-]\d{2}:\d{2})'
	1 octet	Variable	Utilization The current channel utilization measured by the radio on the scanned 20 MHz channel - as defined in section 9.4.2.28 of [1].
	1 octet	Variable 221 - 224: Reserved.	Noise An indicator of the average radio noise plus interference power measured on the 20 MHz channel during a channel scan. Encoding as defined as for ANPI in section 11.11.9.4 of [1].
	2 octets	Variable	NumberOfNeighbors The number of neighbor BSS discovered on this channel.
	6 octets	Variable	BSSID The BSSID indicated by the neighboring BSS. EUI-48
	1 octet	0x00 – 0x20: length of SSID byte array 0x21 - 0xFF: Reserved.	SSID Length
	SSID Length octets	Variable	SSID The SSID indicated by the neighboring BSS.
	1 octet	Variable	SignalStrength An indicator of radio signal strength (RSSI) of the Beacon or Probe Response frames of the neighboring BSS as received by the radio measured in dBm. (RSSI is encoded per Table 9-154 of [[1]). Reserved: 221 - 255.
	1 octet	n	Length of Channel Bandwidth field

Field	Length	Value	Description
	n octets	Variable	ChannelBandwidth String indicating the maximum bandwidth at which the neighbor BSS is operating, e.g., "20" or "40" or "80" or "80+80" or "160" MHz.
	bit 7	1: field present 0: field not present	BSS Load Element Present Set to one if the neighboring BSS's Beacons/Probe Responses include a BSS Load Element as defined in section 9.4.2.28 of [1]. Set to 0 otherwise.
	bits 6 -0		Reserved
	1 octet	Variable	ChannelUtilization If "BSS Load Element Present" bit is set to one, this field is present. Otherwise it is omitted. The value of the "Channel Utilization" field as reported by the neighboring BSS in the BSS Load element.
	2 octets	Variable	StationCount If "BSS Load Element Present" bit is set to one, this field is present. Otherwise it is omitted. The value of the "Station Count" field reported by the neighboring BSS in the BSS Load element.
	The above 10 fields are present NumberOfNeighbors times		
	4 octets	Variable	AggregateScanDuration Total time spent performing the scan of this channel in milliseconds.
	bit 7	1: Scan was an Active scan 0: Scan was Passive scan	Scan Type Indicates whether the scan was performed passively or with Active probing.
	bits 6-0		Reserved

17.2.41 Timestamp TLV format

Table 51 provides the definition for the Timestamp TLV.

Table 51. Timestamp TLV

Field	Length	Value	Description
tlvType	1 octet	0xA8	Timestamp TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	Variable	Timestamp Length
	Timestamp Length Octets	Variable	Timestamp The timestamp shall be formatted as a string using the typedef date-and-time string format as defined in section 3 of [1] and shall include time-secfrac and time-offset as defined in section 5.6 of [1]. '\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}\.d+Z [-+]\d{2}:\d{2}''

17.2.42 CAC Request TLV format

Table 52 provides the definition for the CAC Request TLV.

Table 52. CAC Request TLV format

Field	Length	Value	Description
tlvType	1 octet	0xAD	CAC Request TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	r	Number of Radios Number of radios for which a CAC Request is being made.
	6 octets	Variable	Radio Unique Identifier of a radio of the Multi-AP Agent for which a CAC Request is being made.
	1 octet	Variable	Operating Class Operating class to use for performing the CAC, from Table E-4 in Annex E of [1].
	1 octet	Variable	Channel Single channel number in the operating class on which the Multi-AP Agent is being requested to perform a CAC.
	bits 7-5	"000": Continuous CAC "001": Continuous with dedicated radio "010": MIMO dimension reduced "011": Time sliced CAC "011"-"111": Reserved	CAC Method CAC method to be used.
	bits 4-3	"00": Remain on channel and continue to monitor for radar "01": Return the radio that was performing the CAC to its most recent operational configuration. "10"-"11": Reserved	CAC Completion Action CAC Completion Action for Successful CAC.
	bits 2-0		Reserved
The above 6 fields are repeated r-1 times			

17.2.43 CAC Termination TLV format

Table 53 provides the definition for the CAC Termination TLV.

Table 53. CAC Termination TLV format

Field	Length	Value	Description
tlvType	1 octet	0xAE	CAC Termination TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	r	Number of Radios Number of radios for which a CAC termination is being made.
	6 octets	Variable	Radio Unique Identifier of a radio of the Multi-AP Agent for which the CAC Termination is being made.
	1 octet	Variable	Operating Class Operating class of the CAC to be terminated.
	1 octet	Variable	Channel Single channel number of the CAC to be terminated.
	The above three fields are repeated r-1 times		

17.2.44 CAC Completion Report TLV format

Table 54 provides the definition for the CAC Completion Report TLV.

Table 54. CAC Completion Report TLV format

Field	Length	Value	Description
tlvType	1 octet	0xAF	CAC Completion Report TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	r	Number of Radios Number of radios for which a CAC Completion Report is being sent.
	6 octets	Variable	Radio Unique Identifier of a radio of the Multi-AP Agent used for performing the CAC.
	1 octet	Variable	Operating Class Operating class used for performing the CAC, from Table E-4 in Annex E of [1].
	1 octet	Variable	Channel Channel number used for performing the CAC.
	1 octet	0x00: Successful 0x01: Radar detected 0x02: CAC not supported as requested (capability mismatch) 0x03: Radio too busy to perform CAC 0x04: Request was considered to be non-conformant to regulations in the country in which the Multi-AP Agent is operating 0x05: Other error 0x06 - 0xFF: Reserved	CAC Completion Status.
	1 octet	k	Number of Pairs Number of class and channel pairs that radar was detected on. This field shall be set to 0 if radar was not detected.
	1 octet	Variable	Operating Class Detected Operating class to which the radar was detected, from Table E-4 in Annex E of [1]. This field shall be set to 0 if radar was not detected.
	1 octet	Variable	Channel Detected Single channel number in the operating class on which the radar was detected. This field shall be set to 0 if radar was not detected.
	The above 2 fields are repeated k -1 times.		
	The above 7 fields are repeated r-1 times.		

17.2.45 CAC Status Report TLV format

Table 55 provides the definition for the CAC Status Report TLV.

Table 55. CAC Status Report TLV format

Field	Length	Value	Description
tlvType	1 octet	0xB1	CAC Status Report TLV.

Field	Length	Value	Description
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	a	Number of Available Channels Number of channels the Multi-AP Agent indicates as Available Channels.
	1 octet	Variable	Operating Class Operating class of an Available Channel, from Table E-4 in Annex E of [1].
	1 octet	Variable	Channel Channel number of an Available Channel in the given Operating class.
	2 octets	Variable	Minutes Minutes since CAC was completed identifying Available Channel. Set to zero for non-DFS channels.
	Above 3 fields are repeated a-1 times		
	1 octet	n	Number of Pairs Number of class and channel pairs the Multi-AP Agent indicates are on the non-occupancy list due to detection of radar.
	1 octet	Variable	Operating Class Operating class of channel that is in the non-occupancy list, from Table E-4 in Annex E of [1].
	1 octet	Variable	Channel Single channel number in the operating class on which the radar was detected.
	2 octets	Variable	Duration Seconds remaining in the non-occupancy duration for the channel specified by the class and channel pair.
	Above 3 fields are repeated n-1 times		
	1 octet	c	Number of Pairs Number of class and channel pairs that have an active CAC ongoing.
	1 octet	Variable	Operating Class Operating class of channel that has ongoing CAC, from Table E-4 in Annex E of [1].
	1 octet	Variable	Channel Single channel number in the operating class that has an ongoing CAC.
	3 octets	Variable	Countdown Seconds remaining to complete the CAC.
	Above 3 fields are repeated c-1 times		

17.2.46 CAC Capabilities TLV format

Table 56 provides the definition for the CAC Capabilities TLV.

Table 56. CAC Capabilities TLV format

Field	Length	Value	Description
tlvType	1 octet	0xB2	CAC Capabilities TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	2 octets	Variable	Country Code Two-character country code in which the Multi-AP Agent is operating according to ISO 3166 [5]. The characters shall be encoded as UTF-8.

Field	Length	Value	Description
	1 octet	r	Number of Radios. Separate radios shall be specified only to the extent that all radios specified can perform CACs simultaneously. If the value is zero, the agent has no radios that are able to perform a CAC.
	6 octets	Variable	Radio Unique Identifier of the radio.
	1 octet	t	Number of CAC Types Supported Number of types of CAC that the radio can perform. Each type is defined by a method and time to complete. For each type, the classes and channels allowed are enumerated.
	1 octet	0x00: Continuous CAC 0x01: Continuous with dedicated radio 0x02: MIMO dimension reduced 0x03: Time sliced CAC 0x04 - 0xFF: Reserved	CAC method supported.
	3 octets	Variable	Duration Number of seconds required to complete CAC.
	1 octet	c	Number of Operating Classes Number of classes supported for the given method.
	1 octet	Variable	Operating Class Operating class for which the capability is being described, from Table E-4 in Annex E of [1].
	1 octet	f	Number of Channels Number of channels supported in the given operating class.
	1 octet	Variable	Channel Single channel number in the operating for which the capability is being described.
The above field is repeated f-1 times.			
The above 3 fields are repeated c-1 times.			
The above 6 fields are repeated t-1 times.			
The above 8 fields are repeated r-1 times (if r=0, these fields are omitted).			

17.2.47 Multi-AP Profile TLV format

Table 57 provides the definition for the Multi-AP Profile TLV.

Table 57. Multi-AP Profile TLV format

Field	Length	Value	Description
tlvType	1 octet	0xB3	Multi-AP Profile TLV.
tlvLength	2 octets	1	Number of Octets in ensuing field.
tlvValue	1 octet	0x00: Reserved 0x01: Multi-AP Profile-1 0x02: Multi-AP Profile-2 0x03 ~0xFF Reserved	Multi-AP Profile Field. A 1905 device that receives a Multi-AP Profile TLV with a reserved value shall assume the sender implements the same profile implemented by the receiver.

17.2.48 Profile-2 AP Capability TLV format

Table 58 provides the definition for the Profile-2 AP Capability TLV.

Table 58. Profile-2 AP Capability TLV format

Field	Length	Value	Description
tlvType	1 octet	0xB4	Profile-2 AP Capability TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	2 octets		Reserved.
	bits 7-6	0: bytes 1: kibibytes (KiB) 2: mebibytes (MiB) 3: reserved	Byte Counter Units The units used for byte counters when the Multi-AP Agent reports traffic statistics.
	bits 5-0		Reserved
	1 octet	Variable	Max Total Number of VIDs. Max Total Number of unique VIDs the Multi-AP Agent supports.

17.2.49 Default 802.1Q Settings TLV format

Table 59 provides the definition for the Default 802.1Q Settings TLV.

Table 59. Default 802.1Q Settings TLV format

Field	Length	Value	Description
tlvType	1 octet	0xB5	Default 802.1Q Settings TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	2 octets	Variable	Primary VLAN ID.
	bits 7-5	Variable	Default PCP.
	bits 4-0		Reserved.

17.2.50 Traffic Separation Policy TLV format

Table 60 provides the definition for the Traffic Separation Policy TLV.

Table 60. Traffic Separation Policy TLV format

Field	Length	Value	Description
tlvType	1 octet	0xB6	Traffic Separation Policy TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	k	Number of SSIDs.
	1 octet	n	Length of SSID name.
	n octets	Variable	SSID name.
	2 octets	0x0000 – 0x0002: Reserved 0x0003 – 0x0FFE 0xFFF – 0xFFFF: Reserved	VLAN ID.
	The above 3 fields are repeated k-1 times.		

17.2.51 Profile-2 Error Code TLV format

Table 61 provides the definition for the Profile-2 Error Code TLV.

Table 61. Profile-2 Error Code TLV format

Field	Length	Value	Description
tlvType	1 octet	0xBC	Profile-2 Error code TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	1 octet	0x00: Reserved 0x01: Reserved 0x02: Reserved 0x03: Default PCP or Primary VLAN ID not provided 0x04: Reserved 0x05: Number of unique VLAN ID exceeds maximum supported 0x06: Reserved. 0x07: Traffic Separation on combined fronthaul and Profile-1 backhaul unsupported 0x08: Traffic Separation on combined Profile-1 backhaul and Profile-2 backhaul unsupported 0x09: Reserved. 0x0A – 0xFF: Reserved.	Reason code.
	0 or 6 octets	Variable	BSSID this error refers to. This field shall be included if the Reason code field is set to '0x07' or '0x08'.

17.2.52 AP Radio Advanced Capabilities TLV format

Table 62 provides the definition for the AP Radio Advanced Capabilities TLV.

Table 62. AP Radio Advanced Capabilities TLV format

Field	Length	Value	Description
tlvType	1 octet	0xBE	AP Radio Advanced Capabilities TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique Identifier of the radio for which capabilities are reported.
	bit 7	0 or 1	Combined Front Back Traffic Separation on combined fronthaul and Profile-1 backhaul support.
	bit 6	0 or 1	Combined Profile-1 and Profile-2 Traffic Separation on combined Profile-1 backhaul and Profile-2 backhaul support.
	bit 5-0		Reserved

17.2.53 Association Status Notification TLV format

Table 63 provides the definition for the Association Status Notification TLV.

Table 63. Association Status Notification TLV format

Field	Length	Value	Description
tlvType	1 octet	0xBF	Association Status Notification TLV.
tlvLength	2 octets	variable	Number of octets in ensuing field.
tlvValue	1 octet	k	Number of BSSIDs and their statuses included in this TLV
	6 octets	Any EUI-48 value	BSSID of a BSS operated by the Multi-AP device
	1 octet	0x00: No more associations allowed 0x01: Associations allowed 0x02 – 0xFF: Reserved	Association Allowance status The status of allowance of new client device associations on the BSSs specified by the BSSIDs in this TLV.
	The above 2 fields are repeated k times.		

17.2.54 Source Info TLV format

Table 64 provides the definition for the Source Info TLV.

Table 64. Source Info TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC0	Source Info TLV.
tlvLength	2 octets	6	Number of octets in ensuing field.
tlvValue	6	Any EUI-48 value	MAC Address The MAC address of the device that generated the message included in the tlvValue field of the Tunneled TLV.

17.2.55 Tunneled message type TLV format

Table 65 provides the definition for the Tunneled message type TLV.

Table 65. Tunneled message type TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC1	Tunneled message type TLV.
tlvLength	2 octets	1	Number of octets in ensuing field.
tlvValue	1 octet	0x00: Association Request 0x01: Re-Association Request 0x02: BTM Query 0x03: WNM Request 0x04: ANQP request for Neighbor Report 0x05-0xFF: Reserved	Tunneled Protocol Type 802.11 request frame type carried in the Tunneled TLV.

17.2.56 Tunneled TLV format

Table 66 provides the definition for the Tunneled TLV.

Table 66. Tunneled TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC2	Tunneled TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	Variable	Variable	802.11 request frame body.

17.2.57 Profile-2 Steering Request TLV format

Table 67 provides the definition for the Profile-2 Steering Request TLV.

Table 67. Profile-2 Steering Request TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC3	Profile-2 Steering Request TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	BSSID. Unique identifier of the source BSS for which the steering request applies (i.e. BSS that the STAs specified in the request are currently associated with).
	bit 7	0: Request is a Steering Opportunity. 1: Request is a Steering Mandate to trigger steering for specific client STA(s)	Request Mode.
	bit 6	Variable	BTM Disassociation Imminent bit.
	bit 5	Variable	BTM Abridged bit.
	bits 4-0	0	Reserved.
	2 octets	Variable	Steering Opportunity window. Time period in seconds (from reception of the Steering Request message) for which the request is valid. If Request Mode bit is set to 1, then the value of this field is ignored.
	2 octets	Variable	BTM Disassociation Timer. Time period in TUs of the disassociation timer in the BTM Request.
	1 octet	k = 0: Steering request applies to all Agile Multiband capable associated STAs in the BSS per policy setting. k > 0: Steering request applies to specific Agile Multiband capable STAs specified by STA MAC address(es)	STA List Count k.
	6 octets	Variable	MAC Address Agile Multiband capable STA MAC address for which the steering request applies. If k is 0, then this field is not included.
	The above field is repeated k – 1 times (if k = 0, the above field is omitted).		

Field	Length	Value	Description
	1 octet	m = 1 or k	Target BSSID List Count. If Request Mode bit is set to one and if: m = 1: The same target BSSID is indicated for all specified STAs m = k (k>1): An individual target BSSID is indicated for each specified STA (in the same order) If Request Mode bit is 0, then this field is set to zero.
	6 octets	Variable	Target BSSID. Indicates a target BSSID for steering. Wildcard BSSID is represented by FF:FF:FF:FF:FF:FF.
	1 octet	Variable	Target BSS Operating Class. If the Target BSSID is set to "Wildcard BSSID", the value of this field is ignored by the receiver.
	1 octet	Variable	Target BSS Channel Target BSS Channel Number for channel on which the Target BSS is transmitting Beacon frames. If the Target BSSID is set to "Wildcard BSSID", the value of this field is ignored by the receiver.
	1 octet	Variable	Reason Code Reason code for steering as specified in Table 18 of [8].
	The above 4 fields are repeated m – 1 times (if m = 0, these fields are omitted).		

17.2.58 Unsuccessful Association Policy TLV format

Table 68 provides the definition for the Unsuccessful Association Policy TLV.

Table 68. Unsuccessful Association Policy TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC4	Unsuccessful Association Policy TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	bit 7	0: Do not report unsuccessful association attempts 1: Report unsuccessful association attempts	Report Unsuccessful Associations Indicates whether Multi-AP Agent should report unsuccessful association attempts of client STAs to the Multi-AP Controller
	bits 6-0		Reserved
	4 octets	Variable	Maximum Reporting Rate Maximum rate for reporting unsuccessful association attempts (in attempts per minute)

17.2.59 Metric Collection Interval TLV format

Table 69 provides the definition for the Metric Collection Interval TLV.

Table 69. Metric Collection Interval TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC5	Metric Collection Interval TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.

Field	Length	Value	Description
tlvValue	4 octets	Variable	Collection Interval Device.CollectionInterval as defined in Table 3 & Table 6 of [10]. Note: If a Multi-AP Agent is polled for metrics once every Collection Interval, at least one metric from one radio on the Multi-AP Agent will have been freshly re-measured. Polling more frequently may not provide additional new information.

17.2.60 Radio Metrics TLV format

Table 70 provides the definition for the Radio Metrics TLV.

Table 70. Radio Metrics TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC6	Radio Metrics TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique Identifier of a radio of the Multi-AP Agent for which metrics are being reported.
	1 octet	Variable	Noise Radio.Noise as Table 3 & Table 6 of [10].
	1 octet	Variable	Transmit Radio.Transmit as defined in Table 3 & Table 6 of [10].
	1 octet	Variable	ReceiveSelf Radio.ReceiveSelf as defined in Table 3 & Table 6 of [10].
	1 octet	Variable	ReceiveOther Radio.ReceiveOther as defined in Table 3 & Table 6 of [10].

17.2.61 AP Extended Metrics TLV format

Table 71 provides the definition for the AP Extended Metrics TLV.

Table 71. AP Extended Metrics TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC7	AP Extended Metrics TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	BSSID BSSID of a BSS for which metrics are being reported.
	4 octets	Variable	UnicastBytesSent BSS.UnicastBytesSent as defined in Table 3 & Table 6 of [10], except that the byte counters are encoded in units specified by the Byte Counter Units field of the Profile-2 AP Capability TLV.
	4 octets	Variable	UnicastBytesReceived BSS.UnicastBytesReceived as defined in Table 3 & Table 6 of [10], except that the byte counters are encoded in units specified by the Byte Counter Units field of the Profile-2 AP Capability TLV.
	4 octets	Variable	MulticastBytesSent BSS.MulticastBytesSent as defined in Table 3 & Table 6 of [10], except that the byte counters are encoded in units specified by the Byte Counter Units field of the Profile-2 AP Capability TLV.

Field	Length	Value	Description
	4 octets	Variable	MulticastBytesReceived BSS.MulticastBytesReceived as defined in Table 3 & Table 6 in [10], except that the byte counters are encoded in units specified by the Byte Counter Units field of the Profile-2 AP Capability TLV.
	4 octets	Variable	BroadcastBytesSent BSS.BroadcastBytesSent as defined in Table 3 & Table 6 in [10], except that the byte counters are encoded in units specified by the Byte Counter Units field of the Profile-2 AP Capability TLV.
	4 octets	Variable	BroadcastBytesReceived BSS.BroadcastBytesReceived as defined in Table 3 & Table 6 in [10], except that the byte counters are encoded in units specified by the Byte Counter Units field of the Profile-2 AP Capability TLV.

17.2.62 Associated STA Extended Link Metrics TLV format

Table 72 provides the definition for the Associated STA Extended Link Metrics TLV.

Table 72. Associated STA Extended Link Metrics TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC8	Associated STA Extended Link Metrics TLV.
tlvLength	2 octets	Variable	Number of Octets in ensuing field.
tlvValue	6 octets	Any EUI-48 value	MAC Address of the associated STA.
	1 octet	k (≥ 0)	Number of BSSIDs reported for this STA.
	6 octets	Any EUI-48 value	BSSID of the BSS to which the STA is associated.
	4 octets	Variable	LastDataDownlinkRate STA.LastDataDownlinkRate as defined in Table 3 & Table 6 of [10].
	4 octets	Variable	LastDataUplinkRate STA.LastDataUplinkRate as defined in Table 3 & Table 6 of [10].
	4 octets	Variable	UtilizationReceive STA.UtilizationReceive as defined in Table 3 & Table 6 of [10].
	4 octets	Variable	UtilizationTransmit STA.UtilizationTransmit as defined in Table 3 & Table 6 of [10].
	The above 5 fields are repeated k – 1 times (if k = 0, these fields are omitted).		

17.2.63 Status Code TLV format

Table 73 provides the definition for the Status Code TLV.

Table 73. Status Code TLV format

Field	Length	Value	Description
tlvType	1 octet	0xC9	Status Code TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	2 octets	Variable	Status Code This field shall be set in accordance with Table 9-46 of [1].

17.2.64 Reason Code TLV format

Table 74 provides the definition for the Reason Code TLV.

Table 74. Reason Code TLV format

Field	Length	Value	Description
tlvType	1 octet	0xCA	Reason Code TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	2 octets	Variable	Reason Code This field shall be set in accordance with Table 9-45 of [1].

17.2.65 Backhaul STA Radio Capabilities TLV format

Table 75 provides the definition for the Backhaul STA Radio Capabilities TLV.

Table 75. Backhaul STA Radio Capabilities TLV format

Field	Length	Value	Description
tlvType	1 octet	0xCB	Backhaul STA Radio Capabilities TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	Radio Unique Identifier of the radio for which capabilities are reported.
	bit 7	0: the MAC address is not included below 1: the MAC address is included below	The MAC address include.
	bits 6-0	0	Reserved.
	6 octets	Any EUI-48 value	MAC address of the backhaul STA on this radio. (This field is present if the MAC address include field is set to 1).

17.2.66 Backhaul BSS Configuration TLV

Table 76 provides the definition for the Backhaul BSS Configuration TLV.

Table 76. Backhaul BSS Configuration TLV format

Field	Length	Value	Description
tlvType	1 octet	0xD0	Backhaul BSS Configuration TLV.
tlvLength	2 octets	Variable	Number of octets in ensuing field.
tlvValue	6 octets	Variable	BSSID BSSID of BSS to which this configuration applies.
	bit 7	0: allowed 1: disallowed	Profile-1 bSTA Disallowed Profile-1 Backhaul STA association disallowed.
	bit 6	0: allowed 1: disallowed	Profile-2 bSTA Disallowed Profile-2 Backhaul STA association disallowed.
	bits 5-0		Reserved.

18 Multi-AP Profiles

A Multi-AP device shall implement all the mandatory functionalities in sections, sub-sections and in Table 77, as per the Multi-AP Profile it indicates in any Multi-AP Profile TLV (see 17.2.47) and Multi-AP Profile subelement (see Table 8) it sends.

A Multi-AP device includes a Multi-AP Profile TLV in every 1905 Topology Query message, 1905 Topology Response message, and 1905 AP-Autoconfiguration Search message it sends. If a Multi-AP device does not include a Multi-AP Profile TLV in any of those messages, the device implements only Profile-1.

Additionally, a Multi-AP Controller includes a Multi-AP Profile TLV in every 1905 AP-Autoconfiguration Response message it sends. If a Multi-AP Controller does not include a Multi-AP Profile TLV in any AP-Autoconfiguration Response message it sends, the Controller implements only Profile-1.

A Multi-AP Agent includes a Multi-AP Profile subelement in every (Re)-Association Request and Responses it sends. If a Multi-AP Agent does not include a Multi-AP Profile subelement in any of those frames, the Multi-AP Agent implements only Profile-1.

If a Multi-AP device receives any of the aforementioned messages or frames that includes a Multi-AP Profile TLV or a Multi-AP Profile subelement, with the Multi-AP Profile field set to a reserved value, it shall assume that the sender of such a message or frame implements the same profile implemented by the recipient.

A backhaul link between two Multi-AP devices is said to be a "Profile-X Backhaul", where "X" is the lowest of the profiles implemented by the two devices.

An "X" in Table 77 indicates the profile(s) for which the function applies to.

Table 77. Profile Section Applicability

Function	Section	Applicable to Multi-AP:	
		Profile-1	Profile-2
Multi-AP Onboarding	5	X	X
Multi-AP Discovery	Table 4	X	X
Multi-AP Profile	6.1, 6.2, 17.2.47, 18		X
Multi-AP Configuration	7	X	X
Channel selection	8.1, 8.2	X	X
Co-ordinated CAC	8.1, 8.2.1, 9.1		X
AP Capability	9.1	X	X
Client Capability	9.2	X	X
Link metric collection	10.1, 10.2.1, 10.3, 10.4	X	X
Data element support	6.3, 7.3, 9.1, 10.2, 10.2.1, 10.3.1		X
Channel scan	7.3, 9.1, 10.2.2		X
Client steering	11	X	X
Wi-Fi Agile Multiband and tunneled message support	11.4, 11.5, 11.7		X
Backhaul optimization	12	X	X
Backhaul optimization by backhaul stations association control	12.1		X
Multi-AP messaging security	13	X	X
Four-address MAC header format	14	X	X

Function	Section	Applicable to Multi-AP:	
		Profile-1	Profile-2
Multi-AP control messaging reliability	15	X	X
Higher layer data payload over 1905	16	X	X
Traffic separation general	7.1, 19		X
Traffic separation in presence of Multi-AP Agents with different capabilities	7.1, 7.2, 12.1		X
Multi-AP message format	17	See Table 9	See Table 9

19 Traffic Separation

19.1 Traffic Separation in Multi-AP Network

19.1.1 Traffic Separation Overview (Informative)

This informative description of traffic separation relies on terms defined in section 3.1.

A Multi-AP Controller is able to configure multiple fronthaul SSIDs in a Multi-AP network. A Multi-AP Profile-2 Network Segment supports traffic separation for each fronthaul SSIDs using a unique VLAN. The traffic belonging to each VLAN is distinguished using an 802.1Q C-TAG with a unique VLAN ID, or the lack of thereof.

The rules defined in section 19.1.3 ensure that traffic generated within a Multi-AP network is clearly identifiable as belonging to one SSID. Traffic generated outside of a Multi-AP network is tagged with a VLAN ID (or untagged as appropriate) prior to ingressing the Multi-AP network by means not defined in this specification and is expected to be identified as belonging to an SSID.

A Multi-AP device is a layer-2 (Link Layer) logical device that can be embedded into a more complex physical device (e.g., a router, or a gateway) that implements both a Multi-AP Agent as well as other, above layer-2, functionalities. Often in this case, traffic generated outside of the network (e.g., ingressing thru the WAN interface) is classified by the gateway/routing subsystem and tagged (if needed) before being forwarded to the Multi-AP device subsystem. The abstract/logical interface between the Multi-AP subsystem and the rest of the device is considered a Multi-AP Logical Ethernet Interface as per the definition in section 3.1.3 and the rules in section 19.1.3.

If Traffic Separation is not configured on a Multi-AP Agent that implements Profile-2, the Multi-AP Agent might behave in a transparent manner to VLAN tags applied by other entities.

A Multi-AP Controller configures SSID to VLAN ID mapping in a Traffic Separation Policy. Each mapping from one or many SSIDs to one VLAN ID is indicated in a Traffic Separation Policy TLV. The Multi-AP Controller distributes the Traffic Separation Policy to all Multi-AP Agents. It is recommended that a Multi-AP Controller provides each Multi-AP Agent with a complete list of VLAN ID to SSID mappings, including those VLANs that are mapped to SSIDs that are not configured on a given Multi-AP Agent, to enable that traffic on all VLANs is forwarded over backhaul links. Multi-AP Agents report to the Multi-AP Controller the maximum number of VLANs they are able to configure in the Profile-2 AP Capability TLV. A Controller that intends to use more VLANs than those supported on some of the Multi-AP Agents it manages, may rearrange the topology in such a way that traffic for all VLANs downstream of a Multi-AP Agent can be forwarded by such Agent.

For each Ingress Packet, a Multi-AP Agent adds an 802.1Q C-TAG with a VLAN ID as specified in a Traffic Separation Policy.

For each Egress Packet, a Multi-AP Agent removes any 802.1Q C-TAG.

For a packet to be transmitted on a Multi-AP Logical Ethernet Interface, if the VLAN ID in the 802.1Q C-TAG is set to one of the Secondary VLAN IDs, a Multi-AP Agent maintains the 802.1Q C-TAG on those packets.

Multi-AP IEEE 1905.1 management frames are carried in the Primary Network.

A Default 802.1Q Settings TLV identifies a Primary VLAN ID for tagging packets on the Primary Network.

Traffic separation is not supported across a Multi-AP Agent that implements Profile-1. Therefore, a Multi-AP Controller should not configure any SSID that is mapped to a Secondary VLAN ID on any Multi-AP Agent that implements Profile-1 or on any Multi-AP Agent that is downstream of a Multi-AP Agent that implements Profile-1. If the location of the WAN connection in a network managed by a Multi-AP Controller changes (e.g., in order to use a backup WAN connection in the event the main WAN connection fails), the portions of the network where traffic separation is possible may change and the Multi-AP Controller may need to reconfigure the entire network accordingly, including Secondary SSIDs and VLAN(s).

A Multi-AP Controller that reconfigures VLAN(s) in the entire Multi-AP Profile-2 Network Segment may reconfigure the traffic separation policy on the Multi-AP Agents, starting from those at the very end of the data-plane tree topology and finishing at the data-plane root. Failing to do so may result in the inability to deliver reconfiguration CMDUs to downstream Multi-AP Agents due to Primary VLAN ID mismatch. During VLAN reconfiguration data traffic loss may occur.

Figure 5 shows an example network configuration with traffic separation enabled.

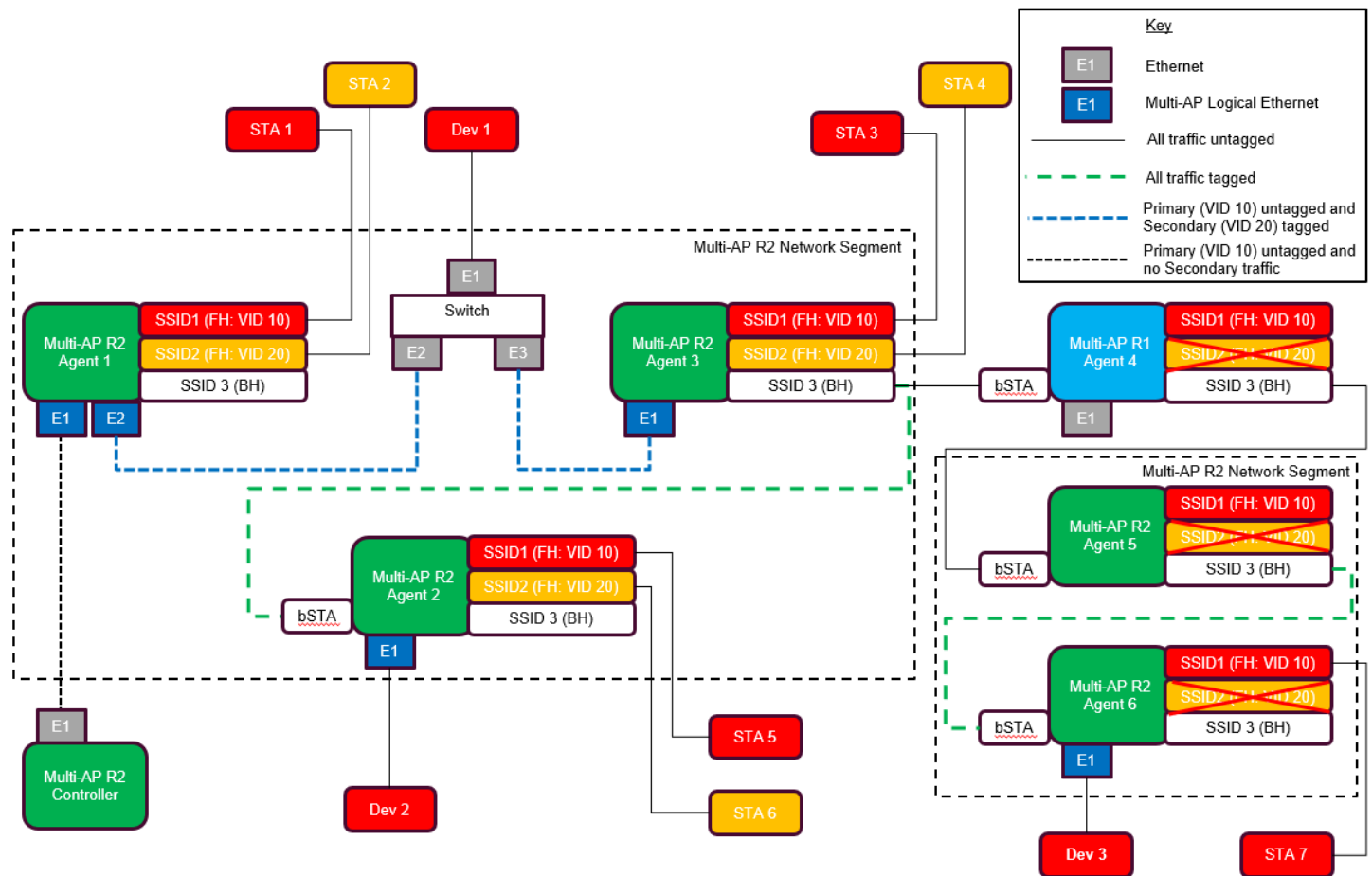


Figure 5. Example Network Configuration with Traffic Separation Enabled

19.1.1.1 Mixed backhaul and fronthaul (Informative)

As a result of the rules detailed in section 19.1.3, when a Multi-AP Agent transmits a packet on a Profile-1 backhaul Wi-Fi Interface, it removes the 802.1Q C-VLAN tag. When a Multi-AP Agent transmits a packet on a Profile-2 backhaul Wi-Fi Interface it maintains the 802.1Q C-VLAN tag. When a BSS on a Multi-AP Agent has been configured as both fronthaul and backhaul BSS, the Multi-AP Agent removes the 802.1Q C-VLAN tag from the packets it transmits to a fronthaul STA.

Some Multi-AP Agent implementations may be able to comply with the requirements described in section 19.1.3, while others may only be able to comply when all of the STAs associated with the same BSS require the same VLAN processing. A Multi-AP Agent indicates its traffic separation capabilities to the Controller within the AP Radio Advanced Capabilities TLV in the 1905 AP-Autoconfiguration WSC message. In a Multi-AP network where Traffic Separation is enabled and a single SSID is used as both fronthaul and backhaul, a Controller that configures a Multi-AP Agent that has reported Combined Front Back bit set to zero might achieve an equivalent topology by configuring this Multi-AP Agent with two BSSs, one used exclusively as fronthaul and one used exclusively as backhaul, both bearing the same SSID and credentials, on the same or on different radios, as permitted by the "Maximum number of BSSs" supported on each of the Multi-AP Agent's radios.

In a Multi-AP network where Traffic Separation is enabled and both Profile-1 and Profile-2 Multi-AP Agents are expected to associate with the backhaul BSS, a Controller that configures a Multi-AP Agent that has reported Combined Profile-1 and Profile-2 bit set to zero might achieve an equivalent topology by configuring this Multi-AP Agent with two backhaul BSSs, both configured as backhaul with same SSID and credentials, one configured with Profile-1 bSTA Disallowed bit

set to one and the other with Profile-2 bSTA Disallowed bit set to one, on the same or on different radios as permitted by the "Maximum number of BSSs" supported on each of the Multi-AP Agent's radios.

Only Multi-AP Agents that report both the aforementioned Profile-1 bSTA Disallowed and Profile-2 bSTA Disallowed bits set to one can be expected to support Traffic separation on a BSS that combine fronthaul and Profile-2 backhaul, or fronthaul and Profile-1 backhaul and Profile-2 backhaul.

In a Multi-AP network where Traffic Separation is enabled and a single SSID is used as both fronthaul and backhaul, and Multi-AP Agents implementing Profile-1 as well as Multi-AP Agents implementing Profile-2 are expected to associate with the backhaul SSID, a Multi-AP Controller that configures an Multi-AP Agent that has reported Combined Front Back bit set to zero, and/or Combined Profile-1 and Profile-2 bit set to zero might achieve an equivalent topology by configuring such Multi-AP Agent with three BSSs, one used exclusively as fronthaul, a second one used exclusively as backhaul with Profile-1 bSTA Disallowed bit set to one, and a third one used exclusively as backhaul with Profile-2 bSTA Disallowed bit set to one. All of the BSSs bear the same SSID and credentials, on the same or on different radios, as permitted by the "Maximum number of BSSs" supported on each of the Multi-AP Agent's radios.

19.1.2 Multi-AP Controller Requirements

A Multi-AP Profile-2 Controller configures Traffic Separation using an AP-Autoconfiguration WSC message or a Multi-AP AP Policy Config Request message or both.

If triggered, a Multi-AP Controller shall send a Traffic Separation Policy TLV to a Multi-AP Agent in a Multi-AP Policy Config Request message.

If a Multi-AP Controller sends a message containing a Traffic Separation Policy TLV that has the Number of SSIDs field set to a non-zero value, it shall include a Default 802.1Q Settings TLV in the message.

If a Multi-AP Controller sends a Traffic Separation Policy TLV to a Multi-AP Agent, it shall send a Traffic Separation Policy TLV that includes a set of unique VIDs that does not exceed the Max Total Number of VIDs reported in the most recent Profile-2 AP Capability TLV received from that Multi-AP Agent.

If a Multi-AP Controller sends a Traffic Separation Policy TLV with the Number of SSIDs field set to a non-zero value to a Multi-AP Agent that has set the Combined Front Back bit and/or the Combined Profile-1 and Profile-2 bit to zero, the Multi-AP Controller should avoid sending a set of BSS configuration and Traffic Separation Policies that the Multi-AP Agent has advertised as unsupported.

Note: Multi-AP Agents that do not report both Combined Front Back bit set to one and Combined Profile-1 and Profile-2 bit set to one may be also unable to support traffic separation on combined fronthaul and Profile-2 backhaul. Agents that do not report both Combined Front Back bit set to one and Combined Profile-1 and Profile-2 bit set to one may be also unable to support traffic separation on combined fronthaul, Profile-1 backhaul and Profile-2 backhaul.

If a Multi-AP Controller sends a Traffic Separation Policy TLV with the Number of SSIDs field set to a non-zero value and one or more M2 TLVs with bit 6 (Backhaul BSS) set to one and SSID assigned a Secondary VLAN ID as per the Traffic Separation Policy TLV, a Multi-AP Agent behavior is unspecified.

If a Multi-AP Controller sends a 1905.1 packet, it shall send it on the Primary Network.

In order to avoid transient misconfiguration, if the Traffic Separation configuration is known to a Multi-AP Controller at the time a new Multi-AP Agent is onboarded, the Multi-AP Controller may include the Traffic Separation Policy TLV and the Default 802.1Q Settings TLV in the onboarding messages (as per section 7.1).

19.1.3 Multi-AP Agent Requirements

If a Multi-AP Agent receives a Multi-AP Policy Config Request message that includes a Traffic Separation Policy TLV, the Multi-AP Agent shall respond with a 1905 Ack message (per section 17.1.32) within one second and before implementing any policy in the received Multi-AP Policy Config Request message.

A Multi-AP Agent may receive a Traffic Separation Policy TLV and a Default 802.1Q Settings TLV in any of the following messages: AP-Autoconfiguration WSC message (see section 7.1), Multi-AP Policy Config Request message (see section 7.3). Additionally, it may receive a Multi-AP Default 802.1Q Setting subelement in (Re-)Association Response frames sent

by Multi-AP Agents that implement Profile-2 (see section 5.2). The subsequent paragraphs in 19.1.3 apply to all the scenarios described above.

If a Multi-AP Agent receives a Traffic Separation Policy TLV that includes a set of VIDs that exceeds the Max Total Number of unique VIDs the Multi-AP Agent supports, the Multi-AP Agent shall send an Error Response message per section 17.1.37 containing one Profile-2 Error Code TLV for each misconfigured BSS with reason code field set to 0x05 per section 17.2.51. If a Multi-AP Agent receives the Traffic Separation Policy TLV in a Multi-AP Policy Config Request message, the Multi-AP Agent shall discard the unsupported policy. If a Multi-AP Agent receives the Traffic Separation Policy TLV in an AP-Autoconfiguration WSC message, the Multi-AP Agent shall tear down the misconfigured BSS, as defined in sections 7.1.

If a Multi-AP Agent is unable to configure one or more BSS as indicated by the received Traffic Separation Policy TLV and the combined fronthaul / Profile-1 backhaul / Profile-2 backhaul configuration, the Multi-AP Agent shall send an Error Response message per section 17.1.37 containing one Profile-2 Error Code TLV for each misconfigured BSS with reason code field set to 0x07 or 0x08 per section 17.2.51. If a Multi-AP Agent receives the Traffic Separation Policy TLV in a Multi-AP Policy Config Request message, the Multi-AP Agent shall discard the unsupported policy. If a Multi-AP Agent receives the Traffic Separation Policy TLV in an AP-Autoconfiguration WSC message, the Multi-AP Agent shall tear down the misconfigured BSS, as defined in section 7.1.

If a Multi-AP Agent has not received a Multi-AP Default 802.1Q Setting subelement in the (Re-)Association Response frame, or a Traffic Separation Policy TLV, or the most recently received Traffic Separation Policy TLV has the Number of SSIDs field set to zero, the Multi-AP Agent shall consider the Primary VLAN ID not configured and may forward VLAN tagged packets received at the Fronthaul interface or Logical Ethernet interface, and shall not add, modify or remove any VLAN tag on any packets it sends or receives and shall not perform traffic separation on the basis of any VLAN tag present in a packet.

If a Multi-AP Agent has received a Traffic Separation Policy and the most recently received Traffic Separation Policy defines at least one SSID to VLAN ID mapping, then it shall perform VLAN tag processing as described below.

If a Multi-AP Agent sends a 1905.1 packet, it shall send it on the Primary Network. If no Primary VLAN ID is configured on this Multi-AP Agent, the Multi-AP Agent shall send these 1905 packets on a Wi-Fi backhaul link without an 802.1Q C-Tag. If a Primary VLAN ID is configured on this Multi-AP Agent, the Multi-AP Agent shall send these packets on a Wi-Fi backhaul link with an 802.1Q C-Tag with VLAN ID equal to the Primary VLAN ID.

If a Multi-AP Agent generates a frame with EtherType 0x888E (EAPOL) on a Profile-2 Wi-Fi backhaul link and no Primary VLAN ID is configured, the Multi-AP Agent shall send these frames without an 802.1Q C-Tag. If a Multi-AP Agent configures a Primary VLAN ID, the Multi-AP Agent shall send EtherType 0x888E frames on a Profile-2 Wi-Fi backhaul link with an 802.1Q C-Tag with VLAN ID equal to the Primary VLAN ID.

Backhaul STA behavior upon (re)association

- If the Backhaul STA of a Multi-AP Agent has successfully associated with a Backhaul BSS whose latest (Re)Association Response frame contains a Multi-AP Default 802.1Q Setting subelement in the Multi-AP IE, with a Primary VLAN ID that differs from the one in use on the newly-associated Agent, or no Primary VLAN ID is configured on the newly-associated Agent, then the newly-associated Agent shall set its Primary VLAN ID to the value contained in the (Re)Association Response frame.
- If the Backhaul STA of a Multi-AP Agent has successfully associated with a Backhaul BSS whose latest (Re)Association Response frame does not contain a Multi-AP Default 802.1Q Setting subelement in the Multi-AP IE and a Primary VLAN ID is configured on the newly-associated Agent, then the newly-associated Agent shall unconfigure its Primary VLAN ID and any Traffic Separation Policy until a Traffic Separation Policy is received from Controller.

If a Multi-AP Agent has learned that the destination address of a packet is on one VLAN and the packet has an 802.1Q C-TAG containing a different VLAN ID, the Multi-AP Agent shall discard the packet.

Wi-Fi Backhaul

- If a Multi-AP Agent receives a packet that is not classified as an Ingress Packet on a Wi-Fi Backhaul Interface (i.e. a Profile-2 backhaul), the Multi-AP Agent shall retain the existing VLAN ID in the 802.1Q C-TAG. A Multi-AP Agent may discard such packets if the 802.1Q C-TAG VLAN ID is not included in the most recently received Traffic Separation Policy TLV

- If a Multi-AP Agent receives a packet that is classified as an Ingress Packet on a Wi-Fi Backhaul Interface (i.e. a Profile-1 backhaul), the Multi-AP Agent shall add an 802.1Q C-TAG onto the packet and set the VLAN ID to the Primary VLAN ID as specified in the Default 802.1Q Settings TLV.
- If a Multi-AP Agent sends a packet that is not classified as an Egress Packet on a Wi-Fi Backhaul Interface (i.e. a Profile-2 backhaul), the Multi-AP Agent shall retain the existing 802.1Q C-TAG, leaving the VLAN ID unmodified.
- If a Multi-AP Agent sends a packet that is classified as an Egress Packet on a Wi-Fi Backhaul Interface (i.e. a Profile-1 backhaul), the Multi-AP Agent shall remove the 802.1Q C-TAG on the packet.

Wi-Fi Fronthaul

- If a Multi-AP Agent receives a packet on a Wi-Fi Fronthaul Interface (i.e. from an associated non-backhaul STA) that has an 802.1Q VLAN Tag, it shall discard that packet.
- If a Multi-AP Agent receives a packet on a Wi-Fi Fronthaul Interface (i.e. from an associated non-backhaul STA) without an existing 802.1Q VLAN Tag, the Multi-AP Agent shall add an 802.1Q C-TAG onto the packet. If the SSID of the Wi-Fi Fronthaul Interface is present in the Traffic Separation Policy TLV, the Multi-AP Agent shall tag the VLAN ID field with the VLAN ID specified in that VLAN ID field in the Traffic Separation Policy TLV that corresponds to the SSID of the Wi-Fi Fronthaul Interface. If the SSID of the Wi-Fi Fronthaul Interface is not present in the Traffic Separation Policy TLV, the Multi-AP Agent shall tag the VLAN ID field with the Primary VLAN ID as specified in the Default 802.1Q Settings TLV.
- If a Multi-AP Agent sends a packet on a Wi-Fi Fronthaul Interface (i.e. to an associated non-backhaul STA), the Multi-AP Agent shall map the PCP field in the 802.1Q C-TAG to WMM (as specified in [12]) and then remove the 802.1Q C-TAG.

Multi-AP Logical Ethernet

- If a Multi-AP Agent receives a packet on a Multi-AP Logical Ethernet Interface and the packet does not have an 802.1Q VLAN Tag, the Multi-AP Agent shall add an 802.1Q C-TAG, setting the VLAN ID to the Primary VLAN ID and the PCP value to the Default PCP value specified in the Default 802.1Q Settings TLV.
- If a Multi-AP Agent receives a packet on a Multi-AP Logical Ethernet Interface and the packet has an 802.1Q VLAN Tag and the first 802.1Q VLAN Tag in the packet is an 802.1Q C-TAG that contains a C-VID value of the Primary VLAN ID as specified in the Default 802.1Q Settings TLV, then the Multi-AP Agent shall not forward it on that same interface, with or without a VLAN tag.
- If a Multi-AP Agent receives a packet on a Multi-AP Logical Ethernet Interface and the packet does not have an 802.1Q VLAN Tag, the Multi-AP Agent shall not forward it on that same interface, with or without a VLAN tag.
- If a Multi-AP Agent receives a packet on a Multi-AP Logical Ethernet Interface and the packet has an 802.1Q VLAN Tag and the first 802.1Q VLAN Tag in the packet is an 802.1Q C-TAG that contains a C-VID value of a Secondary VLAN ID as specified in the Traffic Separation Policy, then the Multi-AP Agent shall retain the 802.1Q C-TAG.
- If a Multi-AP Agent receives a packet on a Multi-AP Logical Ethernet Interface and the packet has an 802.1Q VLAN Tag and the first 802.1Q VLAN Tag is an 802.1Q C-TAG that contains a C-VID that is not listed in the Traffic Separation Policy, the Multi-AP Agent shall discard the packet.
- If a Multi-AP Agent receives a packet on a Multi-AP Logical Ethernet Interface and the packet has an 802.1Q VLAN Tag and the first 802.1Q VLAN Tag is not an 802.1Q C-TAG, the Multi-AP Agent shall either discard the packet or strip the 802.1Q tag that is not a C-TAG and apply the rules described in this section to the resulting packet.
- If a Multi-AP Agent sends a packet on a Multi-AP Logical Ethernet Interface and the packet has an 802.1Q C-TAG that contains a C-VID value of the Primary VLAN ID, the Multi-AP Agent shall remove that 802.1Q C-TAG. If a Multi-AP Agent sends a packet on a Multi-AP Logical Ethernet Interface and the packet has an 802.1Q C-TAG that contains a C-VID value of a Secondary VLAN ID, the Multi-AP Agent shall retain that 802.1Q C-TAG.

19.2 VLAN Tagging in Multi-AP

A Multi-AP Agent applies 802.1Q C-TAGs as described below.

If a Multi-AP Agent includes an 802.1Q C-TAG in an IEEE 802.11 frame, the Multi-AP Agent shall insert the tag as the first and only VLAN tag following the SNAP Extension header as shown in Figure 6.

802.11 Header	802.2 LLC Header			SNAP Extension		802.1Q C-VLAN Tag			<u>EtherType</u>	Payload	FCS
	DSAP (0xAA)	SSAP (0xAA)	Control (0x03)	OUI (0x00-00-00)	Protocol ID (0x8100)	PCP	DEI	VID			

Figure 6. IEEE 802.11 frame with 802.1Q C-TAG

If a Multi-AP Agent includes an 802.1Q C-TAG in an Ethernet frame, the Multi-AP Agent shall insert the tag as the first and only VLAN tag following the source MAC address as shown in Figure 7.

Preamble	SFD	Destination MAC	Source MAC	802.1Q C-VLAN Tag				<u>EtherType</u>	Payload	CRC/FCS
				TPID (0x8100)	PCP	DEI	VID			

Figure 7. Ethernet frame with 802.1Q C-TAG

If a Multi-AP Agent includes an 802.1Q C-TAG in a frame, it shall set the Drop Eligible Indicator (DEI) bit to 0.

Appendix A (Informative) Miscellaneous

A.1 Higher layer protocol field definition (see 16)

Table 78 lists the values that are reserved for the 1-octet higher layer protocol field.

Table 78. Higher layer protocol field definition

Value	Definition
0x00	Reserved.
0x01	TR-181 transport protocol.
0x02 – 0xFF	Reserved.

A.2 Indication of associated 802.11 clients

When a Multi-AP Agent sends a Topology Response message per [1], the non-1905 neighbor device list TLV may be reporting all MAC addresses it has observed that do not also indicate a 1905 AL MAC address. This might include 802.11 clients directly associated with one of the BSS(s) operated by the Multi-AP Agent as well as “behind” 802.11 clients which are connected through another Multi-AP Agent that is connected to this Multi-AP device. As a result, the recipient of the non-1905 neighbor device list TLV in a Topology Response message might not be able to determine the exact Multi-AP device a given 802.11 client is associated with based on this message. The Associated Clients TLV in the 1905 Topology Response message allows a Multi-AP Agent to unequivocally indicate which 802.11 clients are directly associated to each BSS operating on that Multi-AP device.

A.3 Implementation Notes (Informative)

A.3.1 Traffic Separation

Implementers of Multi-AP Controllers managing networks where Traffic Separation is enabled and where Agents are daisy chained (over Wi-Fi or Ethernet backhaul) are reminded that, in order to maintain traffic separation across those backhaul links, a traffic separation policy containing all VIDs in use in the entire network should be sent to each Agent, even where those Agents are not configured to support the corresponding fronthaul SSIDs.

Note that, depending on the max number of VIDs advertised by such an Agent, some topologies may not be properly supported, and a topology change through Backhaul optimization and/or BSS reconfiguration may be necessary.

Implementers of Multi-AP Agents are reminded that the Agents may receive Traffic Separation policies containing SSID to VLAN ID mappings for SSIDs that are not configured on the Agent.

Implementers of Multi-AP Agents are reminded that a BSS will receive both tagged and untagged EAPOL (0x888E) frames (e.g., when Traffic Separation is configured and the same BSS is configured to allow association of both Profile-1 and Profile-2 bSTAs). Implementers need to ensure that received EAPOL frames are properly processed by Supplicant/Authenticator irrespective of whether or not they are tagged.

A.3.2 Controller implementation for Policy Set Up

Implementers of Multi-AP Controllers are reminded that correct sequencing of policy messaging to Agents is essential. When changing the Traffic Separation policies on an existing Multi-AP network, Multi-AP Agents topologically furthest from the Controller should be configured before Multi-AP Agents closer to the controller.

A.3.3 Fragmentation of IEEE 1905

Implementers of Multi-AP device should be aware that some Profile-1 devices may send a fragmented CMDU with the lastFragmentIndicator set to zero and an End of Message TLV.

A.3.4 Multi-AP Logical Ethernet Interfaces

A Multi-AP Logical Ethernet Interface is an interface designed to be used for connecting a Multi-AP Agent to other Multi-AP devices. Implementers are reminded that users may also connect other LAN devices to these interfaces. Implementers of Multi-AP Agents should note that not all Logical Ethernet Interfaces are considered to be Multi-AP Logical Ethernet Interfaces. In particular, a WAN interface on a residential gateway would not normally be considered to be a Multi-AP Logical Ethernet Interface, in which case the requirements in this specification (particularly those relating to VLAN processing for Traffic Separation) would not apply. Implementers need to indicate in the certification process which Logical Ethernet Interfaces are to be tested as Multi-AP Logical Ethernet Interfaces.