IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

SOVEREIGN PEAK VENTURES, LLC,	§	
	§	
Plaintiff,	§	
	§	**JURY TRIAL DEMANDED**
v.	§	
	§	
HEWLETT PACKARD ENTERPRISE COMPANY,	§	**C.A. NO. 2:23-cv-00009**
	§	
Defendant.	§	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Sovereign Peak Ventures, LLC ("SPV") files this Original Complaint against Defendant Hewlett Packard Enterprise Company ("Defendant" or "HPE") for infringement of U.S. Patent No. 7,796,512 (the "'512 patent"), U.S. Patent No. 8,045,531 (the "'531 patent"), U.S. Patent No. 8,270,384 (the "'384 patent"), and U.S. Patent No. 8,467,723 (the "'723 patent"), collectively, the "Asserted Patents."

THE PARTIES

1. Sovereign Peak Ventures, LLC is a Texas limited liability company, with a principal place of business in Allen, TX.

2. On information and belief, Defendant Hewlett Packard Enterprise Company ("HPE") is a Delaware corporation that maintains regular and established places of business throughout Texas, for example, at its facilities in this District at 6080 Tennyson Parkway, Suite 400, Plano, TX 75024. HPE is registered to conduct business in the State of Texas and has appointed CT Corporation System, located at 1999 Bryan ST., Ste. 900, Dallas, TX 75201 as its agent for service of process.

3. HPE is a multinational information technology company and develops and sells networking equipment and related supplies. HPE sells its products to customers, including customers in this District, in the enterprise electronics markets.

4. HPE operates and owns the hpe.com website, and markets, offers, distributes, and provides technical support for its computer products throughout the United States including in this District.

5. HPE develops, designs, manufactures, distributes, markets, offers to sell, and/or sells infringing products and services within the United States, including in this District, and otherwise purposefully directs infringing activities to this District in connection with its Plano, Texas office; its hpe.com website; and its other places of business in Texas and the rest of the United States. Defendant participates in the design, development, manufacture, sale for importation into the United States, offers for sale for importation into the United States, importation into the United States, sale within the United States after importation, and offers for sale within the United States after importation, of networking equipment that infringe the Asserted Patents.

6. On information and belief, Defendant is engaged in making, using, selling, offering for sale, and/or importing, and/or inducing its subsidiaries, affiliates, retail partners, and customers in the making, using, selling, offering for sale, and/or importing throughout the United States, including within this District, products, such as networking equipment, accused of infringement.

7. The Asserted Patents were invented by employees of Panasonic Corporation ("Panasonic"). Founded in 1918, Panasonic has been at the forefront of the electronics industry for over a century. Panasonic made numerous innovations in the home appliance, battery, mobile phone, and television industries. Indeed, Panasonic's invention of the "Paper Battery" in 1979 is

widely credited as enabling the compact electronics of today. In 1991, Panasonic released the Mova P, the smallest and lightest mobile phone on the market, which revolutionized the industry by showing the demand for a compact, lightweight device. Panasonic also produced the first wide-format plasma display and developed the first digital television for the U.S. market. Panasonic's history of innovation is also borne out by its intellectual property. Indeed, a search of the USPTO database where the patent assignee is "Panasonic" yields over 27,000 matches.

8. Prior to the filing of the Complaint, SPV attempted to engage HPE and/or its agents in good faith licensing discussions related to the Asserted Patents, including via letter dated April 19, 2022, and thereafter by conducting technical and licensing discussions with employees from HPE's in-house legal department responsible for patent matters. HPE's past and continuing sales of its devices i) willfully infringe the Asserted Patents and ii) impermissibly take the significant benefits of SPV's patented technologies without fair compensation to SPV.

9. Through offers to sell, sales, imports, distributions, and other related agreements to transfer ownership of Defendant's electronics, such as networking equipment, with distributors and customers operating in and maintaining a significant business presence in the U.S. and/or its U.S. subsidiaries Defendants does business in the U.S., the state of Texas, and in this District.

JURISDICTION AND VENUE

10. This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

11. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

12. This Court has personal jurisdiction over HPE in accordance with due process and/or the Texas Long Arm Statute because, in part, HPE "recruits Texas residents, directly or

through an intermediary located in this state, for employment inside or outside this state." TEX. CIV. PRAC. & REM. CODE § 17.042(3).

13. This Court has personal jurisdiction over HPE because HPE has engaged, and continues to engage in continuous, systematic, and substantial activities within this State, including the substantial marketing and sale of products within this State and this District. Furthermore, upon information and belief, this Court has personal jurisdiction over HPE because HPE has committed acts giving rise to SPV's claims for patent infringement within and directed to this District.

14. For example, HPE is subject to personal jurisdiction in this Court because, *inter alia*, it has regular and established places of business in this District, including offices and data centers located at 6080 Tennyson Parkway, Suite 400, Plano, TX 75024. The Collin County Central Appraisal District (CAD) website indicates that HPE owns multiple places of business in this District including property at 2300 Chelsea Blvd., Allen, TX 75013.

15. HPE's offices in the District are regular and established places of business at least because these locations include many members of HPE's important teams, including Engineering, Technical Consultants, Business Managers, IT Managers for Finance Systems, 5G Core Product Management, and Sales Representatives. HPE's website currently lists over a dozen job postings for its Plano office. HPE employees in the District are highly specialized and are important to the operation of HPE.

16. HPE, directly and through its agents, regularly conducts, solicits, and transacts business in this District and elsewhere in Texas, including through its hpe.com website. For example, HPE employs sales and marketing employees that regularly sell, offer to sell, or otherwise distribute networking equipment in this District and elsewhere in Texas.

17. HPE has committed and continues to commit acts of infringement in violation of 35 U.S.C. § 271, and has made, used, marketed, distributed, offered for sale, and sold infringing products in Texas, including in this District, and engaged in infringing conduct within and directed at or from this District. The infringing networking equipment have been and continue to be distributed to and used in this District. HPE's acts cause injury to SPV, including injury suffered within this District.

18. Moreover, on information and belief, HPE has previously litigated patent infringement cases before this Court without contesting jurisdiction and venue.

19. Exercising personal jurisdiction over HPE in this District would not be unreasonable given Defendant's contacts in this District, the interest in this District of resolving disputes related to products sold herein, and the harm that would occur to SPV.

20. In addition, HPE has knowingly induced and continues to knowingly induce infringement within this District by advertising, marketing, offering for sale and/or selling devices pre-loaded with infringing functionality within this District, to consumers, customers, manufacturers, distributors, resellers, partners, and/or end users, and providing instructions, user manuals, advertising, and/or marketing materials which facilitate, direct or encourage the use of infringing functionality with knowledge thereof.

21. Personal jurisdiction also exists specifically over HPE because it, directly or through affiliates, subsidiaries, agents, or intermediaries, transacts business in this State or purposefully directed at this State (including, without limitation, retail stores including Best Buy and Walmart) by making, importing, offering to sell, selling, and/or having sold infringing products within this State and District or purposefully directed at this State or District.

22. Venue is proper in this District under 28 U.S.C. §§ 1391 and 1400(b) because a substantial part of the events or omissions giving rise to the claims occurred in this District, and because HPE has committed acts of infringement in this District and have a regular and established place of business in this District.

23. With respect to the ’512 patent, the Accused Products comprise wireless access points that are configured to support 802.11k/r, where such devices include, but are not limited to, Aruba Indoor APs: 500 Series, 510 Series, 530 Series, 550 Series, 630 Series, 650 Series, 340 Series (802.11ac -Wave 2), 303 Series (802.11ac -Wave 2), Outdoor APs: 518 Series, 560 Series, 560EX Series, 570 Series, 570EX Series, 580 Series, 580EX Series, 360 Series (802.11ac -Wave 2), 370 Series (802.11ac -Wave 2), 370EX Series (802.11ac -Wave 2), Aruba Remote APs: 500H Series, 303 H Series (802.11ac Wave 2); Aruba Instant On APs: Instant On AP22, Instant On AP11 (802.11ac Wave 2), Instant On AP12(802.11ac Wave 2), Instant On AP15 (802.11ac Wave 2), Instant On AP11D (802.11ac Wave 2), Instant On AP17 (802.11ac Wave 2), as well as, their components, and processes related to the same.

24. With respect to the ’531 patent, the Accused Products comprise networking equipment that are configured to use the Aruba Central management platform, such systems include, but are not limited to, systems deployed using the Aruba Mobility controller and Aruba access points.

25. With respect to the ’384 patent, the Accused Products comprise wireless access points that are configured to establish connections with a controller and exchange information about the separation of functions between themselves and the controller, such systems include, but are not limited to AP-567EX, AP-567, AP-565EX, AP-577EX, AP-575EX, AP-577, AP-565, AP-503H, AP-655, AP-635, AP-575, AP-574, AP-518, AP-505H, AP-505, AP-504, AP-555, AP-535,

AP-534, AP-375EX, AP-515, AP-514, AP-387, AP-303P, AP-377EX, AP-377, AP-375, AP-374, AP-345, AP-344, AP-318, AP-303, AP-203H, AP-367, AP-365, AP-303HR, AP-303H, AP-203RP, AP-203R, IAP-305, IAP-304, IAP-207, IAP-335, IAP-334, IAP-315, IAP-314, IAP-325, IAP-324, IAP-277, IAP-228, IAP-205H, 1AP-215, IAP-214, IAP-205, IAP-204, IAP-275, IAP-274, IAP-103, IAP-225, IAP-224, IAP-115, IAP-114, RAP-155P, RAP-155, RAP-109, RAP-108, RAP-3WN, RAP-3WNP.

26. With respect to the '723 patent, the Accused Products comprise LTE-enabled devices that are configured to perform inter-RAT handovers and/or establish a secure tunnel to trusted packet gateways, where such devices include, but are not limited to, the Aruba 9004-LTE Gateway, the Aruba USB LTE Modem, the Aruba SD-WAN Backpack LTE Solution, as well as, their components, and processes related to the same.

27. On information and belief, HPE has placed and continues to place infringing products and/or products that practice infringing processes into the stream of commerce via established distribution channels, with the knowledge and/or intent that those products are and/or will be imported, used, offered for sale, sold, and continue to be sold in the United States and Texas, including in this judicial district. As a result, HPE has, vicariously through and/or in concert with its alter egos, agents, intermediaries, distributors, importers, customers, subsidiaries, and/or consumers, placed the Accused Products into the stream of commerce via established distribution channels with the knowledge and/or intent that those products were sold and continue to be sold in the United States and Texas, including in this judicial district.

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. 7,796,512)

28. Plaintiff incorporates the preceding paragraphs herein by reference.

29. SPV is the assignee of the '512 patent, entitled "Switching source device, switching destination device, high speed device switching system, and signaling method," with ownership of all substantial rights in the '512 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

30. The '512 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '512 patent issued from U.S. Patent Application No. 11/908,354.

31. HPE has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '512 patent in this judicial district and elsewhere in Texas and the United States.

32. HPE designs, develops, manufactures, assembles and markets wireless access points that are configured to support 802.11k/r.

33. HPE directly infringes the '512 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing those Accused Products, their components and processes, and/or products containing the same that incorporate the fundamental technologies covered by the '512 patent.

34. For example, HPE infringes claim 1 of the '512 patent via the Accused Products, which are configured to support 802.11k/r.

35. The Accused Products comprise "a switching source device for moving a session established with a communication counterpart to a switching destination device" that satisfies the limitations of claim 1. For example, the Accused Products support 802.11k/r, such as the Accused Products, act as switching source devices for moving a session with connected clients to switching destination devices, or APs to which the client may choose to roam. Further, the Accused Products

use 802.11r (Fast Basic Service Set (BSS) Transition (FT)), which reduces the latency experienced by AP-roaming clients and allows mobile clients to experience "seamless transitions."

A revision was published in 2012, which incorporated into the 2007 revision the following amendments:

— IEEE Std 802.11k™-2008: Radio Resource Measurement of Wireless LANs (Amendment 1)

— IEEE Std 802.11r™-2008: Fast Basic Service Set (BSS) Transition (Amendment 2)

4.3.11.10 Neighbor report

The neighbor report request is sent to an AP, which returns a neighbor report containing information about known neighbor APs that are candidates for a service set transition. Neighbor reports contain information from dot11RMNeighborReportTable concerning neighbor APs. This request/report pair enables a STA to gain information about the neighbors of the associated AP to be used as potential roaming candidates.

4.5.4.8 Fast BSS transition

The FT mechanism defines a means for a STA to set up security and QoS parameters prior to reassociation to a new AP. This mechanism allows time-consuming operations to be removed from the time-critical reassociation process.

IEEE Std 802.11-2016

36. The Accused Products comprise "a service discovery section for obtaining information as to whether a service can be provided from a neighboring communication device." For example, the Accused Products are configured to use a service discovery section for obtaining the information used to compile a neighbor report.

11.11.10 Usage of the neighbor report

11.11.10.1 General

A neighbor report is sent by an AP and it contains information on neighboring APs that are members of ESSs requested in the neighbor report request. A neighbor report might not be exhaustive either by choice, or due to the fact that there might be neighbor APs not known to the AP. The neighbor report contents are derived from the NeighborListSet parameter of the MLME-NEIGHBORREPRESP.request primitive. The mechanism by which the contents of this table are determined is outside the scope of this standard, but it may include information from measurement reports received from the STAs within the BSS, information obtained via a management interface, or the DS.

The BSSID Information field can be used to help determine neighbor service set transition candidates. It is 4 octets in length and contains the subfields as shown in Figure 9-296.

	B0 B1	B2	B3	B4 B9	B10	B11	B12	B13	B14 B31
	AP Reachability	Security	Key Scope	Capabilities	Mobility Domain	High Throughput	Very High Throughput	FTM	Reserved
Bits:	2	1	1	6	1	1	1	1	18

Figure 9-296—BSSID Information field

The AP Reachability field indicates whether the AP identified by this BSSID is reachable by the STA that requested the neighbor report. For example, the AP identified by this BSSID is reachable for the exchange of preauthentication frames as described in 12.6.10.2. The values are shown in Table 9-150.

	B4	B5	B6	B7	B8	B9
	Spectrum Management	QoS	APSD	Radio Measurement	Delayed Block Ack	Immediate Block Ack
Bits:	1	1	1	1	1	1

Figure 9-297—Capabilities subfield

The Mobility Domain bit is set to 1 to indicate that the AP represented by this BSSID is including an MDE in its Beacon frames and that the contents of that MDE are identical to the MDE advertised by the AP sending the report.

The High Throughput bit is set to 1 to indicate that the AP represented by this BSSID is an HT AP including the HT Capabilities element in its Beacons, and that the contents of that HT Capabilities element are identical to the HT Capabilities element advertised by the AP sending the report.

The Very High Throughput bit is set to 1 to indicate that the AP represented by this BSSID is a VHT AP and that the VHT Capabilities element, if included as a subelement in the report, is identical in content to the VHT Capabilities element included in the AP's Beacon.

9.4.2.39 BSS Average Access Delay element

The BSS Average Access Delay element contains the AP Average Access Delay, which is a measure of load in the BSS and is available in both QoS APs and non-QoS APs. The format of the BSS Average Access Delay element is defined in Figure 9-304.

9.4.2.43 BSS Available Admission Capacity element

The BSS Available Admission Capacity element contains a list of Available Admission Capacity fields at different User Priorities and Access Categories as shown in Figure 9-308.

NOTE—The BSS Available Admission Capacity element is helpful for roaming QoS STAs to select a QoS AP that is likely to accept future admission control requests, but it does not provide an assurance that the HC will admit these requests.

9.4.2.50 RIC Data element (RDE)

The RIC refers to a collection of elements that are used to express a resource request and to convey responses to the corresponding requests.

A RIC is a sequence of one or more Resource Requests, or a sequence of one or more Resource Responses. Each Resource Request or Response consists of an RDE, followed by one or more elements that describe that resource. See 13.11 for examples and procedures.

IEEE Std 802.11-2016

Further, the service discovery section may obtain information about neighboring communication devices from measurement reports or from background scans. Further, the ability of the Accused Products to conduct load balancing and band steering operations among clients and other HPE-Aruba APs is evidence that these Accused Products are aware of their RF environment.

AP Load Balancing ArubaOS: Load balancing

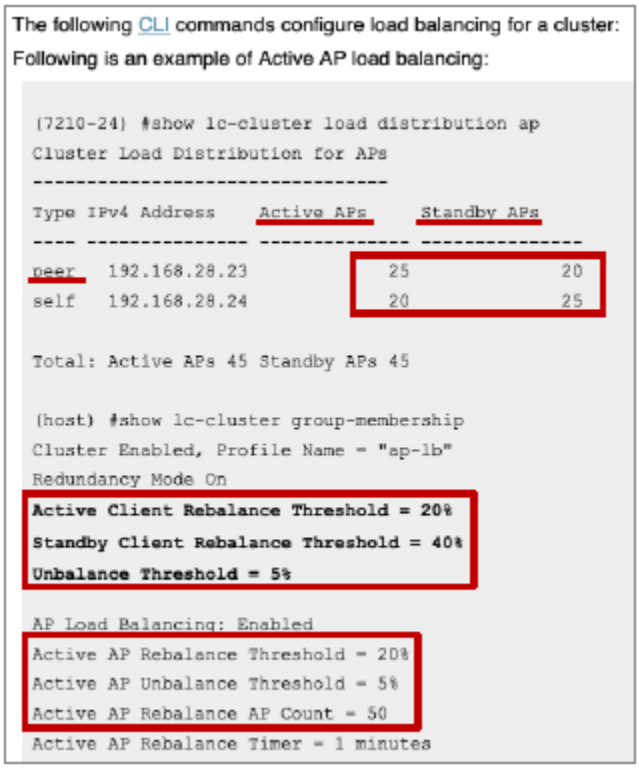
The AP load balancing feature ensures that the cluster leader manages the load balancing based on the platform capacity. The AP is dynamically assigned an AAC when it connects to a cluster. Here, instead of client load, AP load is considered.

Both active and standby APs are considered for load balancing.

Following is the AP load balancing criteria if a managed device is newly added:

- When an AP threshold is already met in the cluster nodes, if a new managed device is added, the Active AP table of the new managed device is filled first based on AP count set.
- When the threshold is not met, APs are moved to standby AP table of the newly added managed device.
- The count of these APs will increment based on the AP count set only after the stabilization of the cluster, however, the APs that were moved during this phase cannot be always based on AP Count.

```
Cluster Info Table
------------------
Type IPv4 Address     Priority Connection-Type  STATUS
---- ---------------- -------- ---------------  ------
self 192.168.10.38    128      N/A              CONNECTED (Leader)
peer 192.168.10.34    128      L2-Connected     CONNECTED (Member, last HBT_RSP 38ms ago, RTD= 0.000 ms)
```



The following CLI commands configure load balancing for a cluster:

Following is an example of Active AP load balancing:

```
(7210-24) #show lc-cluster load distribution ap
Cluster Load Distribution for APs
---------------------------------
Type IPv4 Address    Active APs     Standby APs
---- --------------- -------------- ---------------
peer   192.168.28.23          25              20
self   192.168.28.24          20              25

Total: Active APs 45 Standby APs 45

(host) #show lc-cluster group-membership
Cluster Enabled, Profile Name = "ap-lb"
Redundancy Mode On
Active Client Rebalance Threshold = 20%
Standby Client Rebalance Threshold = 40%
Unbalance Threshold = 5%

AP Load Balancing: Enabled
Active AP Rebalance Threshold = 20%
Active AP Unbalance Threshold = 5%
Active AP Rebalance AP Count = 50
Active AP Rebalance Timer = 1 minutes
```

37. The Accused Products comprise "a high speed device switching section for instructing the service discovery section at an arbitrary timing to inquire whether a service can be provided, determining a switching destination candidate device that is a switching destination of a session based on the obtained information as to whether the service can be provided, generating a switching destination candidate device list describing the switching destination candidate devices, and making an instruction for establishing a session with the switching destination candidate device." For example, the Accused Products are configured to instruct their respective service discovery sections to inquire whether a service can be provided by requesting beacon reports from connected clients at arbitrary times.

11.11.9 Specific measurement usage

11.11.9.1 Beacon report

If a STA accepts a Beacon request it shall respond with a Radio Measurement Report frame containing Beacon reports for all observed BSSs matching the BSSID and SSID in the Beacon request, at the level of detail requested in the Reporting Detail. If the Reporting Detail is 1 and the optional Request subelement is

9.4.2.21.7 Beacon request

The Measurement Request field corresponding to a Beacon request is shown in Figure 9-156.

Operating Class	Channel Number	Randomization Interval	Measurement Duration

The Randomization Interval field specifies the upper bound of the random delay to be used prior to making the measurement, in units of TUs. See 11.11.3.

The Measurement Duration field is set to the preferred or mandatory duration of the requested measurement, in units of TUs. See 11.11.4.

IEEE Std 802.11-2016

The Accused Products are configured to determine switching destination candidate APs using information obtained by the service discovery sections. This determination may be made based on the BSSID of a known AP, or based on information relating to an AP's settings and capabilities.

The BSSID is the BSSID of the BSS being reported. The subsequent fields in the Neighbor Report element pertain to this BSS.

The BSSID Information field can be used to help determine neighbor service set transition candidates. It is 4 octets in length and contains the subfields as shown in Figure 9-296.

B0 B1	B2	B3	B4 B9	B10	B11	B12	B13	B14 B31
AP Reachability	Security	Key Scope	Capabilities	Mobility Domain	High Throughput	Very High Throughput	FTM	Reserved
Bits: 2	1	1	6	1	1	1	1	18

Figure 9-296—BSSID Information field

IEEE Std 802.11-2016

The Accused Products are configured to generate a neighbor list, describing the switching candidate APs.

The following MLME primitives support the signaling of neighbor report responses.

6.3.33.2 MLME-NEIGHBORREPRESP.request

Name	Type	Valid range	Description
NeighborListSet	Set of Neighbor List elements each as defined in the Neighbor Report element format	As defined in 9.4.2.37	A set of Neighbor List elements, each representing a neighboring AP being reported as defined in the Neighbor Report element format.
VendorSpecificInfo	A set of elements	As defined in 9.4.2.26	Zero or more elements.

IEEE Std 802.11-2016

The Accused Products are configured to make an instruction for establishing a session with the switching destination candidate device. For example, the Neighbor Report element for each neighbor contains the AP's respective BSSID, which is used to subsequently establish a Fast Transition session with that AP.

The target AP and the current AP need to reside in the same mobility domain to successfully exchange Remote Request frames. The RRB on the current AP shall transmit Remote Request frames to the target AP based on the BSSID of the target AP (supplied in the FT Action frames) using the same procedures as preauthentication, as described in 12.6.10.2.

Element ID	Length	BSSID	BSSID Information	Operating Class	Channel Number	PHY Type	Optional Subelements
1	1	6	4	1	1	1	variable

Figure 9-295—Neighbor Report element format

9.6.9.2 FT Request frame

The FT Request frame is sent by the STA to its associated AP to initiate an over-the-DS fast BSS transition.

Figure 9-688 shows the format of the FT Request frame Action field.

	Category	FT Action	STA Address	Target AP Address	FT Request frame body
Octets:	1	1	6	6	variable

Figure 9-688—FT Request frame Action field format

The Category field is defined in 9.4.1.11.

The FT Action field is defined in 9.6.9.1.

The STA Address field is set to the fast BSS transition originator's (FTO's) MAC address.

The Target AP Address field is set to the BSSID value of the target AP.

IEEE Std 802.11-2016

38. The Accused Products comprise "a signaling section for establishing a session with the switching destination candidate device when the instruction for establishing a session is received from the high speed device switching section." For example, the Remote Request Broker (RRB) of an Accused Product establishes a session, over the DS, with the switching destination candidate device (target AP).

distribution system (DS): A system used to interconnect a set of basic service sets (BSSs) and integrated local area networks (LANs) to create an extended service set (ESS).

13.10.2 Remote request broker (RRB)

The RRB resides in the SME on the APs and acts as a forwarding agent (at the current AP) and termination point (at the target AP) for protocol messages over the DS.

The RRB allows APs that are part of the same mobility domain to exchange information over the DS. APs that advertise the same MDID shall be reachable over the DS and support the over-the-DS communication.

As a termination point, when the RRB at the target AP receives a request frame from the current AP, it interacts with the MAC and other parts of the SME to process the request and respond with a Remote Response frame, through the RRB on the current AP, back to the requesting FTO.

As a forwarding agent, when the RRB at the current AP receives a request from an FTO directed to another AP in the same mobility domain, the current AP forwards the request to that target AP. The RRB on the

IEEE Std 802.11-2016

39. The Accused Products comprise "an input section for receiving a switching destination candidate device list request from a user." For example, the Accused Products include an input section for receiving, e.g., neighbor report requests from connected users' devices.

11.11.10.3 Responding to a neighbor report request

If dot11RMNeighborReportActivated is true, an AP receiving a neighbor report request shall respond with a Neighbor Report Response frame containing zero or more Neighbor Report elements. If an SSID element is

IEEE Std 802.11-2016

40. The Accused Products comprise "an output section for presenting the switching destination candidate device list when the high speed device switching section receives the switching destination candidate device list request through the input section. For example, the

Accused Products include an output section for presenting the neighbor report to a connected client, in response to a neighbor report request.

4.3.11.10 Neighbor report

The neighbor report request is sent to an AP, which returns a neighbor report containing information about known neighbor APs that are candidates for a service set transition. Neighbor reports contain information from dot11RMNeighborReportTable concerning neighbor APs. This request/report pair enables a STA to gain information about the neighbors of the associated AP to be used as potential roaming candidates.

11.11.10 Usage of the neighbor report

11.11.10.1 General

A neighbor report is sent by an AP and it contains information on neighboring APs that are members of ESSs requested in the neighbor report request. A neighbor report might not be exhaustive either by choice, or due to the fact that there might be neighbor APs not known to the AP. The neighbor report contents are derived from the NeighborListSet parameter of the MLME-NEIGHBORREPRESP.request primitive. The mechanism by which the contents of this table are determined is outside the scope of this standard, but it may include information from measurement reports received from the STAs within the BSS, information obtained via a management interface, or the DS.

IEEE Std 802.11-2016

41. The high-speed device switching section is configured such that when it "receives a device switching request from a user through the input section, it notifies the signaling section of the device selected from the switching candidate device list, and the signaling section sends a switching instruction to the selected device." For example, when an Accused Product receives a switching request (FT Action Request) from a user's device, it sends a Remote Request to the Target AP.

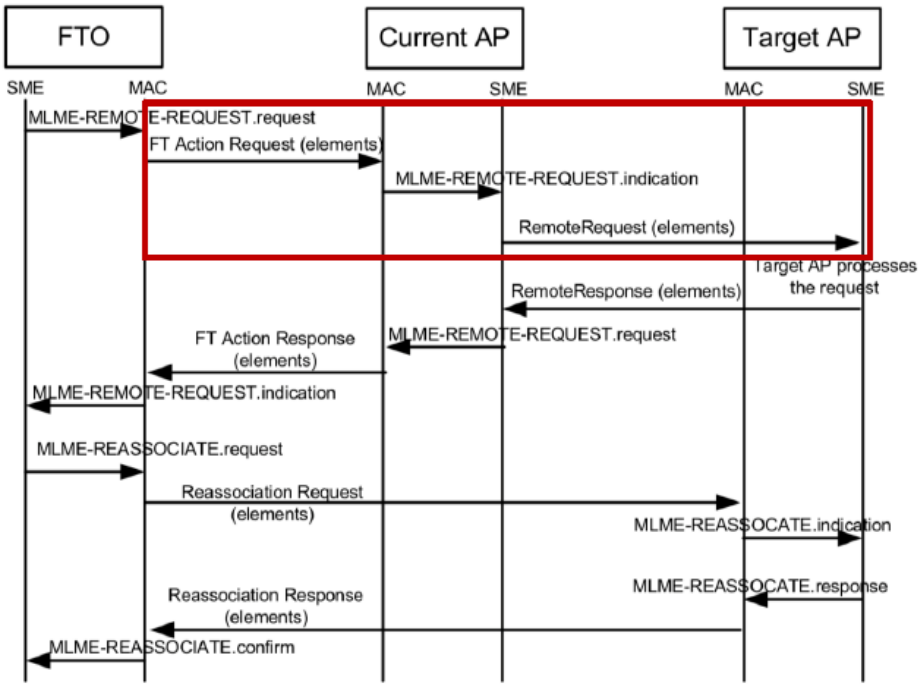


Figure 13-6—MLME interfaces for over-the-DS FT protocol messages

IEEE Std 802.11-2016

The Remote Request message contains a switching instruction, including, e.g., instructions for the robust security network (RSN) association.

robust security network association (RSNA): The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-way handshake or FT protocol. Note that existence of an RSNA between two STAs does not of itself provide robust security. Robust security is provided when all STAs in the network use RSNAs.

13.8 FT authentication sequence

13.8.1 Overview

The FT authentication sequence comprises four sets of FT elements. Each set of FT elements is referred to in 13.8 as a *message*. These messages are included in the FT Protocol frames or FT Resource Request Protocol frames to initiate a fast BSS transition. The FT authentication sequence is always initiated by the FTO and responded to by the target AP.

In an RSN, the first two messages in the sequence allow the FTO and target AP to provide association instance identifiers, SNonce and ANonce, respectively. SNonce and ANonce are chosen randomly or pseudorandomly and are used to generate a fresh PTK. The first two messages also enable the target AP to provision the PMK-R1 and the FTO and target AP to compute the PTK. The third and fourth messages demonstrate liveness of the peer, authenticate the elements, and enable an authenticated resource request.

IEEE Std 802.11-2016

42. The technology discussion above and the exemplary Accused Products provide context for Plaintiff's infringement allegations.

43. At a minimum, HPE has known of the '512 patent at least as early as the filing date of the complaint. In addition, HPE has known about the '512 patent since at least August 19, 2022 when HPE was given access to a data room providing notice of its infringement.

44. On information and belief, since at least the above-mentioned date when HPE was on notice of its infringement, HPE has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the Accused Products that include or are made using all of the limitations of one or more claims of the '512 patent to directly infringe one or more claims of the '512 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, HPE does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '512 patent. HPE intends to cause, and has taken affirmative steps to induce infringement by its distributors, importers, customers, subsidiaries, and/or consumers by at least, inter alia, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing and certifying wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to these purchasers in the United States.

45. In the alternative, on information and belief, since at least the above-mentioned date when HPE was on notice of its infringement, HPE has contributorily infringed, under U.S.C. §

271(c), one or more claims of the '512 patent. For example, HPE contributes to the direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the Accused Products. To the extent that the Accused Products do not directly infringe one or more claims of the '512 patent, such products contain instructions, such as source code, that are especially adapted to cause the Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the Accused Products to provide and utilize neighbor reports in an infringing manner and are a material part of the invention of the '512 patent and are not a staple article of commerce suitable for substantial non-infringing use.

46. On information and belief, despite having knowledge of the '512 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '512 patent, HPE has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. HPE's infringing activities relative to the '512 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

47. SPV has been damaged as a result of HPE's infringing conduct described in this Count. HPE is, thus, liable to SPV in an amount that adequately compensates SPV for HPE's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II

(INFRINGEMENT OF U.S. PATENT NO. 8,045,531)

48. Plaintiff incorporates the preceding paragraphs herein by reference.

49. SPV is the assignee of the '531 patent, entitled "System and method for negotiation of WLAN entity," with ownership of all substantial rights in the '531 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

50. The '531 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '531 patent issued from U.S. Patent Application No. 10/591,184.

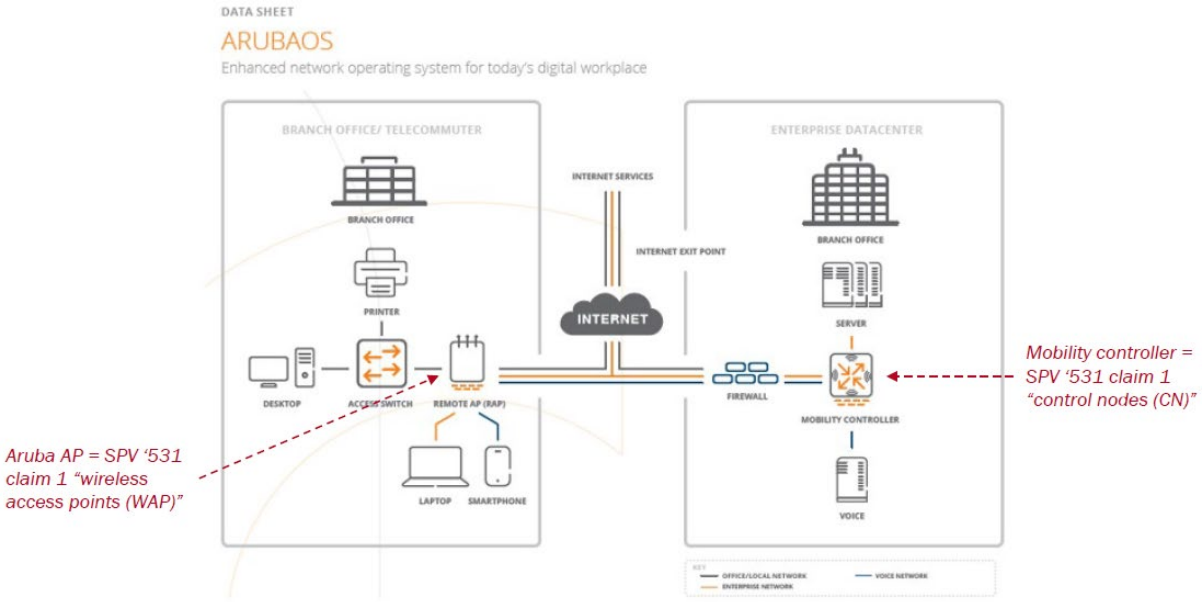
51. HPE has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '531 patent in this judicial district and elsewhere in Texas and the United States.

52. HPE designs, develops, manufactures, assembles and markets networking equipment that is configured to use the Aruba Central management platform.

53. HPE directly infringes the '531 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing those Accused Products, their components and processes, and/or products containing the same that incorporate the fundamental technologies covered by the '531 patent.

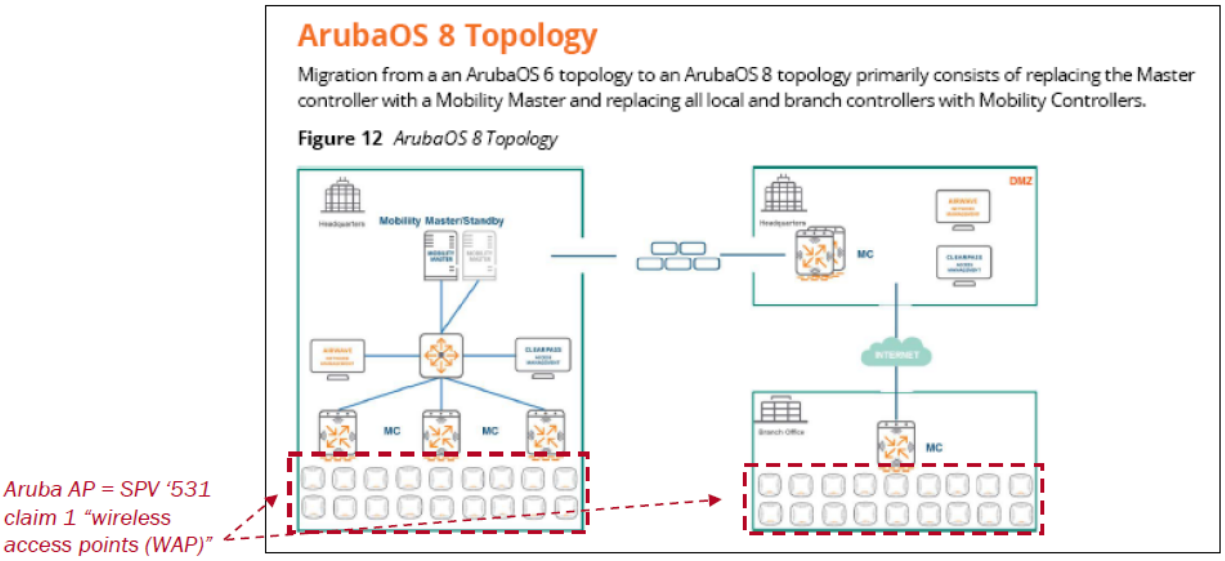
54. For example, HPE infringes claim 1 of the '531 patent via the Accused Products, which are configured to use the Aruba Central management platform.

55. The Accused Products comprise a "system for providing service in a wireless local area network" that satisfies the limitations of claim 1. For example, The Accused Products with Aruba Central-managed access points is a system for providing service in a wireless local area network. The Accused Products are configured such that traffic flows between an Aruba mobility controller (control node) and one or Aruba wireless access points (WAPs).



Source: https://www.arubanetworks.com/assets/ds/DS_ArubaOS.pdf

56. The Accused Products comprise "a single or plurality of wireless access points (WAP) for processing a subset of complete functionality defined for the wireless local area network." For example, the Accused Products comprise one or more controller-managed APs (WAPs). Implicated Aruba AP models include all AP models that can be managed by an Aruba mobility controller (MC) (e.g., 7000 Series (7005, 7008, 7010, 7024, 7030), 7200 Series (7205, 7210, 7220, 7240, 7280), and 9000 Series (9004, 9012)).



Source: https://www.arubanetworks.com/assets/tg/TD_ArubaOS-8-Fundamental-Guide.pdf. In the Accused Products, WLAN functionality is distributed among Aruba mobility controller (control node) and the MC-managed APs. For example, MC-managed APs can be configured by a MC to implement (process) certain client-facing WLAN functions (including, for example, ClientMatch, Air Slice, and Radio Resource Management (802.11k)) that are a subset of complete functionality defined for the WLAN

ClientMatch Capabilities

ClientMatch features a number of capabilities that enable it to pair clients to the desired APs and radios. In general, the following client/AP mismatch conditions are managed by client match:

Band Steering

Dual band clients scan all the channels on both 2.4 GHz and 5 GHz radio and try to connect to the BSSID with the strongest signal or the BSSID that responds first to the client's probe request. This may result in a client connecting to a SSID in 2.4 GHz at lower PHY rates, where as it could have connected to the same SSID in a clear 5 GHz channel with better PHY rates. In such scenarios, the ClientMatch band steers clients to the appropriate band.

The band steering logic of client match continuously monitors a client's association and band steers it to the desired band when appropriate. A clientmatch enabled Aruba AP monitors the clients associated to its 802.11b/g radio and band steers the clients if the following conditions are met:

- The client signal strength on g radio is lower than the band steer g-band min signal (default: -45 dBm)
- The client signal strength on a radio on the same AP is higher than the band steer a-band min signal (default: -75 dBm)

Dynamic Load Balancing

Dynamic Load Balancing enables APs and controllers to dynamically load balance Wi-Fi clients to the APs within the same RF neighborhood on underutilized channels. This technique helps stationary and roaming clients in dense office environments, conference rooms, lecture halls, and environments that have high bandwidth applications as client density to dynamically balance among APs in the same vicinity.

Aruba controller monitors the clients associated to each radio and load balances them if the following conditions are met:

- The client count on a radio is higher than the load balancing client threshold (default: 10)
- The client SNR on a radio with lesser load is higher than the load balancing SNR threshold (default: 30 db).

Sticky Client Steering

Once attached to an AP, many clients tend to stay attached even when users begin to move away from the AP and WLAN signal weakens. As a result of this stickiness, performance for mobile users and clients often degrades, and the overall network throughput deteriorates. ClientMatch steers such sticky clients to a better AP and improves user experience and overall network performance.

Aruba AP monitors the SNR of the clients associated to it and initiates a sticky move if the following conditions are met:

- The client SNR is lesser than the sticky client check SNR (default: 18 db)
- Based on a virtual beacon report, there is a better radio to steer clients to if the following conditions are met:
  - SNR of the target radio is higher than the SNR threshold (default 10 db) and
  - Signal strength of the target radio is equal or higher than Sticky Min Signal (default: -70 dBm)

HOW AIR SLICE WORKS

Air Slice begins to work the moment a user onboards a device to the network. By combining PEF intelligence with Wi-Fi 6 technologies such as OFDMA, MU-MIMO, TWT, and network scheduling, Air Slice allows for flexible Wi-Fi resource management. Here's how it works:

1. **Initial configuration:** IT uses Aruba Central to configure Air Slice policies based on business application requirements, as well as user role and device type on a per-network basis. This is then used to inform SLAs.
2. **Client device onboarding:** An end-user onboards a device to the network, at which point an Aruba AP will provide Air Slice with visibility into the user role, device type, and ongoing application use. Wi-Fi 6 radio resources are automatically allocated based on the client device.
3. **Client uses an application:** An end-user accesses an application recognized by Air Slice, which then assigns radio resources to the application. As new users connect and application sessions begin or end, radio resources change dynamically.

Configuring Radio Resource Management Information Elements

ArubaOS supports the following radio resource management information elements (RRM IEs) for APs with 802.11k support enabled. These settings can be enabled through the WebUI or CLI.

In the WebUI

To select the RRM IEs to be sent in beacons and probe responses using the WebUI:

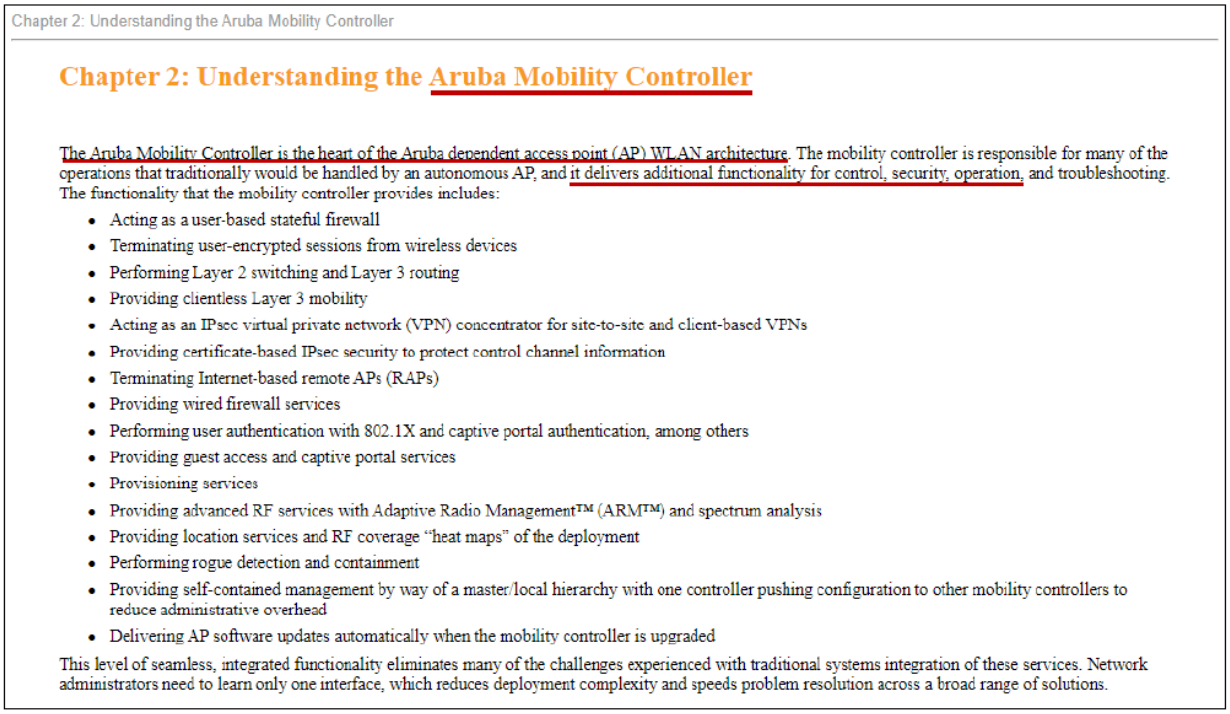
1. Navigate to **Configuration>Advanced Services>All Profile Management**.
2. Expand the **Wireless LAN** menu and select **RRM IE**.
3. Select the RRM IE profile you want to configure, then select any of the following IE types to enable that information element in beacons and probe responses. (All IE types are sent by default.)

Table 2: *RRM IE Parameters*

Parameter	Description
Advertise Enabled Capabilities IE	This value is used to determine if the RRM Enabled Capabilities IE should be advertised in the beacon frames. A value of "Enabled" allows the RRM Enabled Capabilities IE to be present in the beacon frames when 802.11K capability is enabled. A value of "Disabled" prevents the advertisement of the RRM Enabled Capabilities IE in the beacon frames when 802.11K capability is enabled.

57. The Accused Products comprise "a single or plurality of control nodes (CN) for providing a subset or complete functionalities defined for the wireless local area network." For

example, the Accused Products comprises one or more control nodes in the form of Aruba mobility controllers.



Chapter 2: Understanding the Aruba Mobility Controller

Chapter 2: Understanding the Aruba Mobility Controller

The Aruba Mobility Controller is the heart of the Aruba dependent access point (AP) WLAN architecture. The mobility controller is responsible for many of the operations that traditionally would be handled by an autonomous AP, and it delivers additional functionality for control, security, operation, and troubleshooting. The functionality that the mobility controller provides includes:

- Acting as a user-based stateful firewall
- Terminating user-encrypted sessions from wireless devices
- Performing Layer 2 switching and Layer 3 routing
- Providing clientless Layer 3 mobility
- Acting as an IPsec virtual private network (VPN) concentrator for site-to-site and client-based VPNs
- Providing certificate-based IPsec security to protect control channel information
- Terminating Internet-based remote APs (RAPs)
- Providing wired firewall services
- Performing user authentication with 802.1X and captive portal authentication, among others
- Providing guest access and captive portal services
- Provisioning services
- Providing advanced RF services with Adaptive Radio Management™ (ARM™) and spectrum analysis
- Providing location services and RF coverage "heat maps" of the deployment
- Performing rogue detection and containment
- Providing self-contained management by way of a master/local hierarchy with one controller pushing configuration to other mobility controllers to reduce administrative overhead
- Delivering AP software updates automatically when the mobility controller is upgraded

This level of seamless, integrated functionality eliminates many of the challenges experienced with traditional systems integration of these services. Network administrators need to learn only one interface, which reduces deployment complexity and speeds problem resolution across a broad range of solutions.

The functionality is distributed among the Aruba mobility controller ('531 CN) and the managed Aruba APs. For example, the Aruba mobility controllers are configured to provide certain network-facing WLAN functions that are a subset or complete functionalities defined for the WLAN (these network-facing functions include but are not limited to: AirMatch, Web Content Classification, and dynamic load balancing.

AirMatch in ArubaOS 8

AirMatch provides unprecedented quality for RF network resource allocation. It collects data from the past 24 hours of RF network statistics and proactively optimizes the network for the next day.

As a best practice, the RF plan change should be deployed at the time of lowest network utilization so that client disconnects have a minimal impact on user experience. In addition to proactive channel planning done every 24 hours, AirMatch also reacts to dynamic changes in the RF environment such as radar and high noise events. AirMatch results in a stable network experience with greatly minimized channel and EIRP changes. AirMatch is defined by the following key attributes:

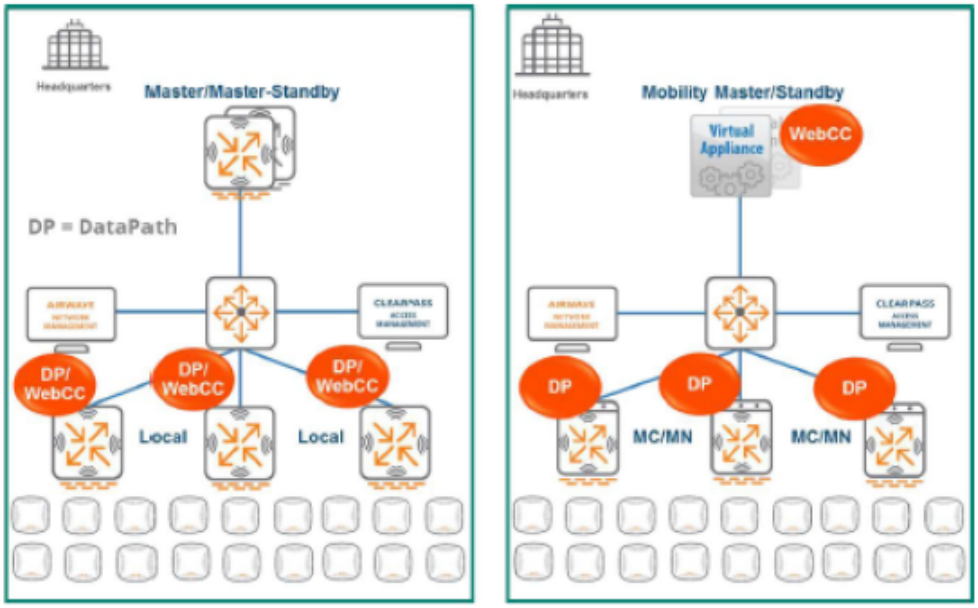
- A centralized RF optimization service
- Newly defined information collection and configuration deployment paths
- Models and solves the network as a whole
- Results in optimal channel, bandwidth, and EIRP plan for the network

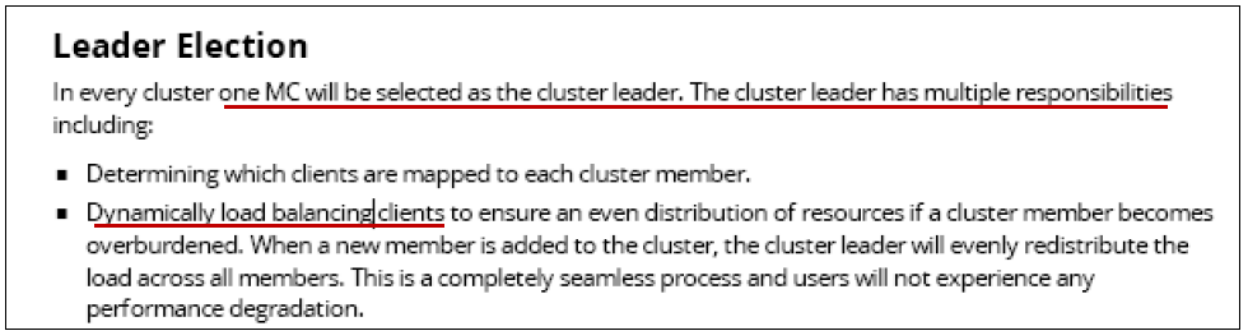
Web Content Classification

Web Content Classification (WebCC) is a feature on Aruba controllers and IAPs that was first introduced in ArubaOS 6. It classifies http and https traffic into category and reputation. Firewall rules can then be applied accordingly based on WebCC's classification. WebCC prevents spyware and malware by blocking access to dangerous and provide visibility into the web content categories and sites being accessed by users.

In an ArubaOS 6 deployment, the WebCC process runs on the local controllers. In ArubaOS 8, the underlying architecture has been changed by moving WebCC process to the Mobility Master in the form of an application or loadable service.

Figure 44 *WebCC Changes in ArubaOS 8*



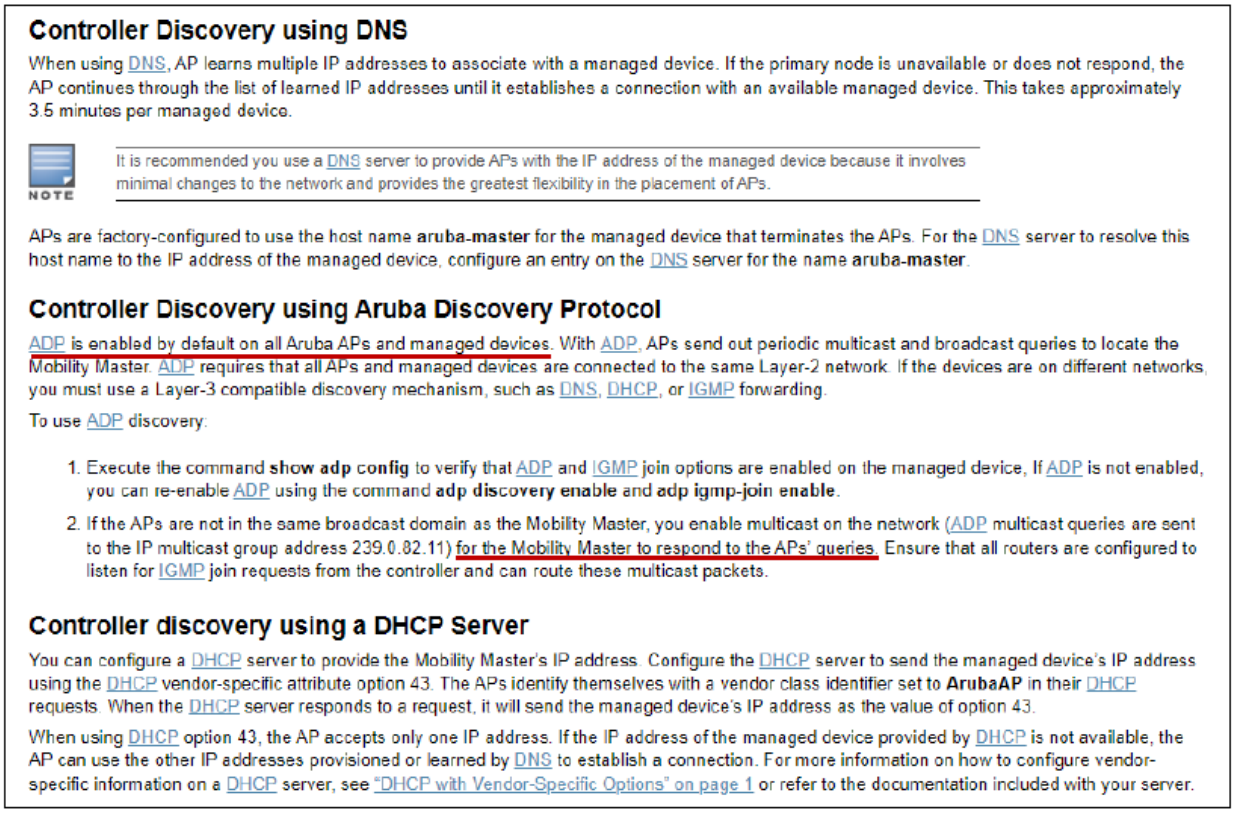


Leader Election

In every cluster one MC will be selected as the cluster leader. The cluster leader has multiple responsibilities including:

- Determining which clients are mapped to each cluster member.
- Dynamically load balancing clients to ensure an even distribution of resources if a cluster member becomes overburdened. When a new member is added to the cluster, the cluster leader will evenly redistribute the load across all members. This is a completely seamless process and users will not experience any performance degradation.

58. The Accused Products comprise "a negotiation unit for the single or plurality of WAPs to dynamically negotiate with the control node for a secure connection and function split arrangement." For example, the access points convey their capabilities to a mobility controller (control node) that will utilize this information to configure the network and establish a secure session. The discovery/response signaling occurs in part via a WAP negotiation.



Controller Discovery using DNS

When using DNS, AP learns multiple IP addresses to associate with a managed device. If the primary node is unavailable or does not respond, the AP continues through the list of learned IP addresses until it establishes a connection with an available managed device. This takes approximately 3.5 minutes per managed device.

NOTE

It is recommended you use a DNS server to provide APs with the IP address of the managed device because it involves minimal changes to the network and provides the greatest flexibility in the placement of APs.

APs are factory-configured to use the host name **aruba-master** for the managed device that terminates the APs. For the DNS server to resolve this host name to the IP address of the managed device, configure an entry on the DNS server for the name **aruba-master**.

Controller Discovery using Aruba Discovery Protocol

ADP is enabled by default on all Aruba APs and managed devices. With ADP, APs send out periodic multicast and broadcast queries to locate the Mobility Master. ADP requires that all APs and managed devices are connected to the same Layer-2 network. If the devices are on different networks, you must use a Layer-3 compatible discovery mechanism, such as DNS, DHCP, or IGMP forwarding.

To use ADP discovery:

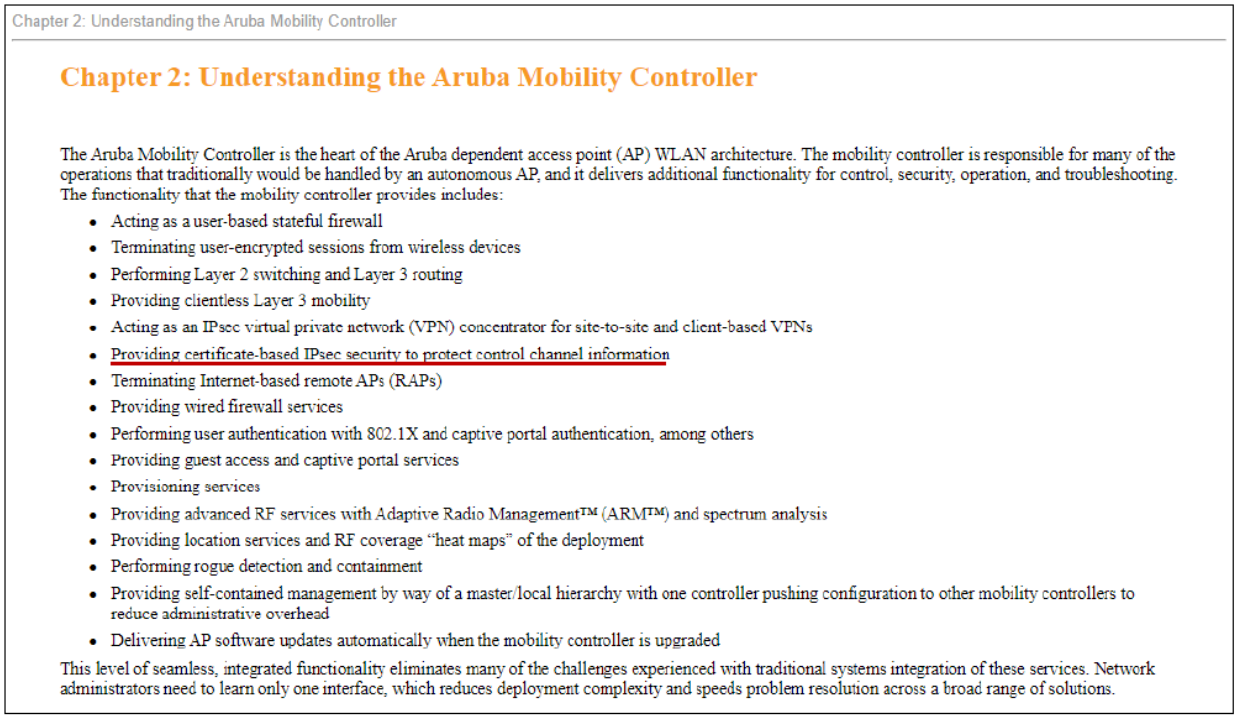
1. Execute the command **show adp config** to verify that ADP and IGMP join options are enabled on the managed device. If ADP is not enabled, you can re-enable ADP using the command **adp discovery enable** and **adp igmp-join enable**.
2. If the APs are not in the same broadcast domain as the Mobility Master, you enable multicast on the network (ADP multicast queries are sent to the IP multicast group address 239.0.82.11) for the Mobility Master to respond to the APs' queries. Ensure that all routers are configured to listen for IGMP join requests from the controller and can route these multicast packets.

Controller discovery using a DHCP Server

You can configure a DHCP server to provide the Mobility Master's IP address. Configure the DHCP server to send the managed device's IP address using the DHCP vendor-specific attribute option 43. The APs identify themselves with a vendor class identifier set to **ArubaAP** in their DHCP requests. When the DHCP server responds to a request, it will send the managed device's IP address as the value of option 43.

When using DHCP option 43, the AP accepts only one IP address. If the IP address of the managed device provided by DHCP is not available, the AP can use the other IP addresses provisioned or learned by DNS to establish a connection. For more information on how to configure vendor-specific information on a DHCP server, see "DHCP with Vendor-Specific Options" on page 1 or refer to the documentation included with your server.

The Accused Products include a secure connection between the control node (Aruba mobility controller) and WAPs (managed Aruba APs). Use of TLS/X.509 certificates involve a negotiation of the parameters of the secure connection.



Chapter 2: Understanding the Aruba Mobility Controller

Chapter 2: Understanding the Aruba Mobility Controller

The Aruba Mobility Controller is the heart of the Aruba dependent access point (AP) WLAN architecture. The mobility controller is responsible for many of the operations that traditionally would be handled by an autonomous AP, and it delivers additional functionality for control, security, operation, and troubleshooting. The functionality that the mobility controller provides includes:

- Acting as a user-based stateful firewall
- Terminating user-encrypted sessions from wireless devices
- Performing Layer 2 switching and Layer 3 routing
- Providing clientless Layer 3 mobility
- Acting as an IPsec virtual private network (VPN) concentrator for site-to-site and client-based VPNs
- Providing certificate-based IPsec security to protect control channel information
- Terminating Internet-based remote APs (RAPs)
- Providing wired firewall services
- Performing user authentication with 802.1X and captive portal authentication, among others
- Providing guest access and captive portal services
- Provisioning services
- Providing advanced RF services with Adaptive Radio Management™ (ARM™) and spectrum analysis
- Providing location services and RF coverage "heat maps" of the deployment
- Performing rogue detection and containment
- Providing self-contained management by way of a master/local hierarchy with one controller pushing configuration to other mobility controllers to reduce administrative overhead
- Delivering AP software updates automatically when the mobility controller is upgraded

This level of seamless, integrated functionality eliminates many of the challenges experienced with traditional systems integration of these services. Network administrators need to learn only one interface, which reduces deployment complexity and speeds problem resolution across a broad range of solutions.

Further, the discovery and AP/network confirmation process involves the Aruba mobility controller and the Aruba AP negotiating a functional split arrangement (i.e. which functions are handled by the control node and WAPs respectively).

Masters are responsible for the following functions in the WLAN:

- **Policy configuration**: Configuration in the Aruba solution is split between policy and local configurations. Local configuration relates to physical interfaces, IP networking, and VLANs, which are different for each mobility controller. Policy configuration is centered on the operation of APs and users, including AP settings such as the SSID name, encryption, regulatory domain, channel, power, and ARM settings. Policy configuration extends beyond APs and also covers user authentication, firewall policy, mobility domains (IP mobility), IPsec, and system management. The policy is pushed to all locals in the form of profiles, and profiles combine to create the configuration for the dependent APs.
- **AP white lists:** Two types of white lists exist in the system, one for RAPs and one for CAPs that use CPsec. These lists determine which APs can connect to the mobility controllers. Unauthorized devices are prevented from connecting to the network.
- **Wireless security coordination:** Wireless intrusion prevention activities involve looking for rogue (unauthorized) APs and monitoring for attacks on the WLAN infrastructure or clients. The master processes all data collected by Aruba APs and AMs. Instructions to disable a rogue AP or blacklist a client from the network are issued through the master.
- **Valid AP list:** All mobility controllers in the network must also know all legitimate APs that operate on the WLAN. These APs must be added to the valid AP list. This list prevents valid APs from being falsely flagged as rogue APs. This is important when APs that are attached to two different locals are close enough to hear each other's transmissions. The valid AP list helps ARM to differentiate between APs that belong to the network and those that are neighbors.

  Unlike traditional wireless intrusion detection system (WIDS) solutions, the master controller automatically generates the valid AP list without network administrator intervention. All Aruba APs are automatically learned and added to the list, but valid third-party APs must be added manually. If more than one master/local cluster exists, AirWave should be deployed to coordinate APs between clusters.
- **RF visualization:** The Aruba RF visualization tools provide a real-time view of the network coverage. This information is based on the AP channel and power settings and the data collected from AMs and APs listening to transmissions during their scanning periods. This information provides a real-time picture of the RF coverage as heard by the APs.
- **Location:** Locating users in the WLAN is more difficult with mobile clients and IP mobility. The IP address of the client is no longer synonymous with location. The Aruba WLAN scans off of the configured channel, so it is possible to hear clients operating on other channels. This information can then be used to triangulate users and rogue devices to within a small area. This information is displayed on the master and allows for devices to be located quickly. This speed is critically important for physical security and advanced services such as E911 calling.
- **Initial AP configuration:** When an AP first boots up, it contacts its master to receive the configuration generated by the master. The master compares the AP information and determines its group assignment, and then redirects that AP to the proper local.
- **Control plane security:** When CPsec is enabled, the master generates the self-signed certificate and acts as the certificate authority (CA) for the network. The master issues certificates to all locals in the network, which in turn certify APs. If more than one master exists in the network, the network administrator assigns a single master as the trust anchor for that network. The trust anchor issues certificates to the other master controllers in the network.
- **Authentication and roles:** User authentication methods and role assignments are created on the master and then propagated to locals throughout the network. A database exists to authenticate users in small deployments or for guest access credentials that can be leveraged by all the mobility controllers in the network. Additionally, the master can proxy requests for the network to a RADIUS or LDAP server.

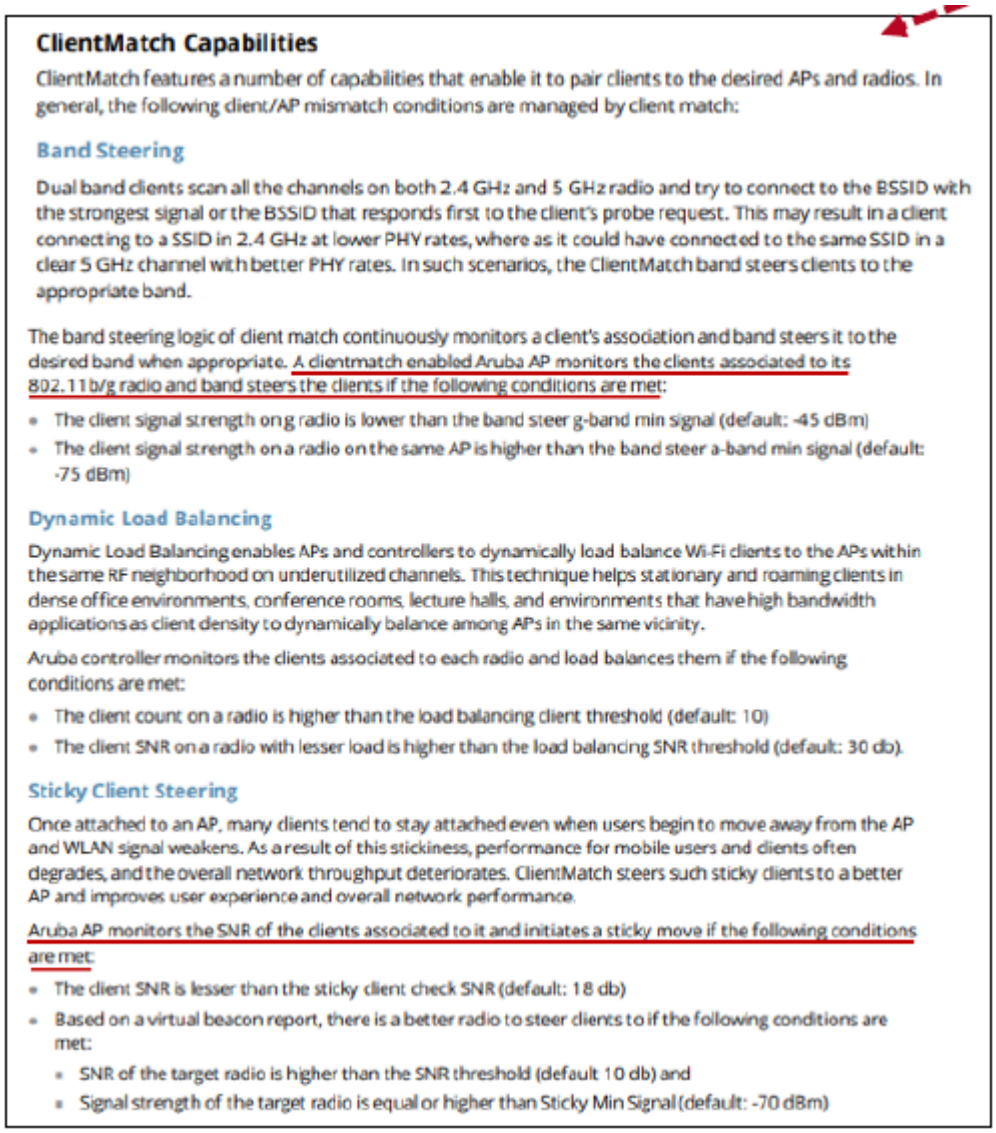
59. The control node is configured such that it "negotiates with the single or plurality of WAPs using the negotiation unit and provides complementary functionality for the single or plurality of each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision of the negotiation unit." For example, the Aruba mobility controller (control node) provides complimentary functionality for the APs by, for example, providing the networking-facing functions used by the APs—this network-facing functionality forming a complete WLAN functionality with the APs' client-facing functionality. Further, Functions of an Insight managed WLAN are split between those functions performed by the mobility controller and separate functions performed by the managed APs.

Chapter 2: Understanding the Aruba Mobility Controller

The Aruba Mobility Controller is the heart of the Aruba dependent access point (AP) WLAN archite
operations that traditionally would be handled by an autonomous AP, and it delivers additional functi
The functionality that the mobility controller provides includes:

- Acting as a user-based stateful firewall
- Terminating user-encrypted sessions from wireless devices
- Performing Layer 2 switching and Layer 3 routing
- Providing clientless Layer 3 mobility
- Acting as an IPsec virtual private network (VPN) concentrator for site-to-site and client-base
- Providing certificate-based IPsec security to protect control channel information
- Terminating Internet-based remote APs (RAPs)
- Providing wired firewall services
- Performing user authentication with 802.1X and captive portal authentication, among others
- Providing guest access and captive portal services
- Provisioning services
- Providing advanced RF services with Adaptive Radio Management™ (ARM™) and spectrur
- Providing location services and RF coverage "heat maps" of the deployment
- Performing rogue detection and containment
- Providing self-contained management by way of a master/local hierarchy with one controller reduce administrative overhead
- Delivering AP software updates automatically when the mobility controller is upgraded

This level of seamless, integrated functionality eliminates many of the challenges experienced with t
administrators need to learn only one interface, which reduces deployment complexity and speeds pr



ClientMatch Capabilities

ClientMatch features a number of capabilities that enable it to pair clients to the desired APs and radios. In general, the following client/AP mismatch conditions are managed by client match:

Band Steering

Dual band clients scan all the channels on both 2.4 GHz and 5 GHz radio and try to connect to the BSSID with the strongest signal or the BSSID that responds first to the client's probe request. This may result in a client connecting to a SSID in 2.4 GHz at lower PHY rates, where as it could have connected to the same SSID in a clear 5 GHz channel with better PHY rates. In such scenarios, the ClientMatch band steers clients to the appropriate band.

The band steering logic of client match continuously monitors a client's association and band steers it to the desired band when appropriate. A clientmatch enabled Aruba AP monitors the clients associated to its 802.11b/g radio and band steers the clients if the following conditions are met:

- The client signal strength on g radio is lower than the band steer g-band min signal (default: -45 dBm)
- The client signal strength on a radio on the same AP is higher than the band steer a-band min signal (default: -75 dBm)

Dynamic Load Balancing

Dynamic Load Balancing enables APs and controllers to dynamically load balance Wi-Fi clients to the APs within the same RF neighborhood on underutilized channels. This technique helps stationary and roaming clients in dense office environments, conference rooms, lecture halls, and environments that have high bandwidth applications as client density to dynamically balance among APs in the same vicinity.

Aruba controller monitors the clients associated to each radio and load balances them if the following conditions are met:

- The client count on a radio is higher than the load balancing client threshold (default: 10)
- The client SNR on a radio with lesser load is higher than the load balancing SNR threshold (default: 30 db).

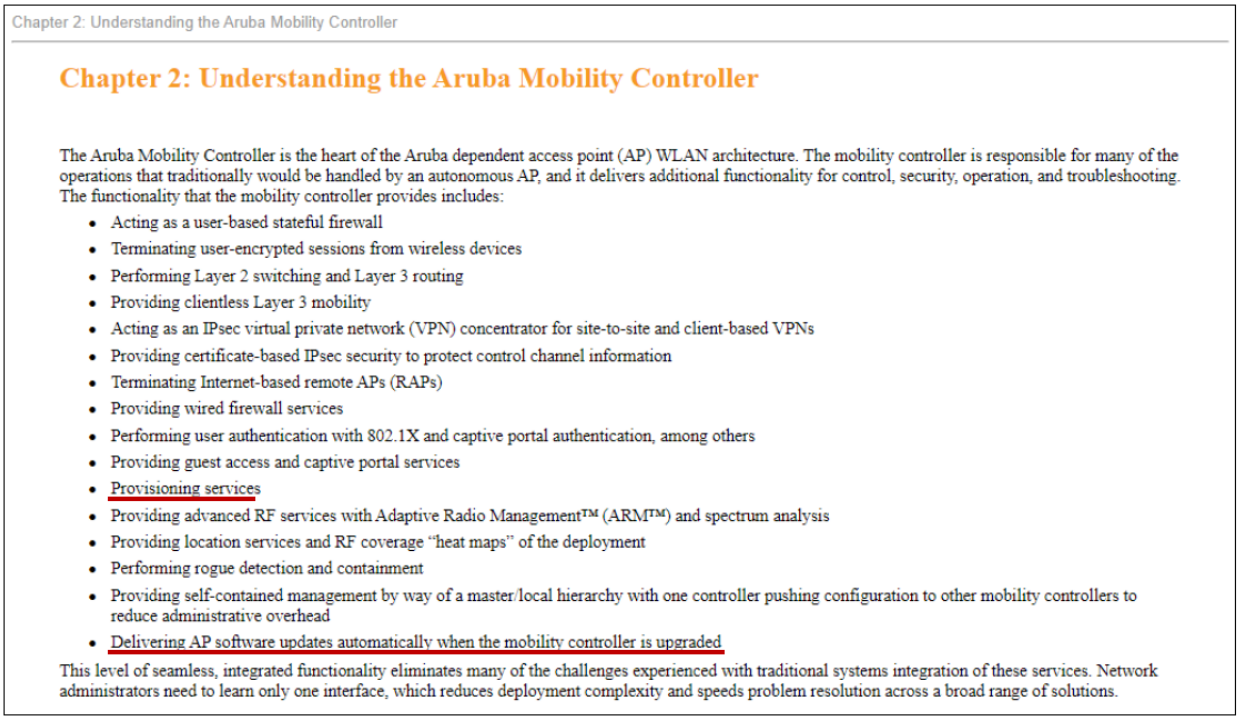
Sticky Client Steering

Once attached to an AP, many clients tend to stay attached even when users begin to move away from the AP and WLAN signal weakens. As a result of this stickiness, performance for mobile users and clients often degrades, and the overall network throughput deteriorates. ClientMatch steers such sticky clients to a better AP and improves user experience and overall network performance.

Aruba AP monitors the SNR of the clients associated to it and initiates a sticky move if the following conditions are met:

- The client SNR is lesser than the sticky client check SNR (default: 18 db)
- Based on a virtual beacon report, there is a better radio to steer clients to if the following conditions are met:
  - SNR of the target radio is higher than the SNR threshold (default 10 db) and
  - Signal strength of the target radio is equal or higher than Sticky Min Signal (default: -70 dBm)

Separately, the Aruba mobility controller also provides complimentary functionality for the APs by, for example, managing the APs provisioning, configuration, and operation—this network wide management functionality forming a complete WLAN functionality with the AP-specific operational functionality (e.g., running a specific config, specific firmware, etc).



Chapter 2: Understanding the Aruba Mobility Controller

Chapter 2: Understanding the Aruba Mobility Controller

The Aruba Mobility Controller is the heart of the Aruba dependent access point (AP) WLAN architecture. The mobility controller is responsible for many of the operations that traditionally would be handled by an autonomous AP, and it delivers additional functionality for control, security, operation, and troubleshooting. The functionality that the mobility controller provides includes:

- Acting as a user-based stateful firewall
- Terminating user-encrypted sessions from wireless devices
- Performing Layer 2 switching and Layer 3 routing
- Providing clientless Layer 3 mobility
- Acting as an IPsec virtual private network (VPN) concentrator for site-to-site and client-based VPNs
- Providing certificate-based IPsec security to protect control channel information
- Terminating Internet-based remote APs (RAPs)
- Providing wired firewall services
- Performing user authentication with 802.1X and captive portal authentication, among others
- Providing guest access and captive portal services
- Provisioning services
- Providing advanced RF services with Adaptive Radio Management™ (ARM™) and spectrum analysis
- Providing location services and RF coverage "heat maps" of the deployment
- Performing rogue detection and containment
- Providing self-contained management by way of a master/local hierarchy with one controller pushing configuration to other mobility controllers to reduce administrative overhead
- Delivering AP software updates automatically when the mobility controller is upgraded

This level of seamless, integrated functionality eliminates many of the challenges experienced with traditional systems integration of these services. Network administrators need to learn only one interface, which reduces deployment complexity and speeds problem resolution across a broad range of solutions.

60. The technology discussion above and the exemplary Accused Products provide context for Plaintiff's infringement allegations.

61. At a minimum, HPE has known of the '531 patent at least as early as the filing date of the complaint. In addition, HPE has known about the '531 patent since at least August 19, 2022, when HPE was given access to a data room providing notice of its infringement.

62. On information and belief, since at least the above-mentioned date when HPE was on notice of its infringement, HPE has actively induced, under U.S.C. § 271(b), distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the Accused Products that include or are made using all of the limitations of one or more claims of the '531 patent to directly infringe one or more claims of the '531 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, HPE does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '531 patent. HPE intends to cause, and has taken affirmative steps

to induce infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to these purchasers in the United States.

63. In the alternative, on information and belief, since at least the above-mentioned date when HPE was on notice of its infringement, HPE has contributorily infringed, under U.S.C. § 271(c), one or more claims of the '531 patent. For example, HPE contributes to the direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the Accused Products. To the extent that the Accused Products do not directly infringe one or more claims of the '531 patent, such products contain instructions, such as source code, that are especially adapted to cause the Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the Accused Products to provide and utilize the Aruba Central management platform in an infringing manner and are a material part of the invention of the '531 patent and are not a staple article of commerce suitable for substantial non-infringing use.

64. On information and belief, despite having knowledge of the '531 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '531 patent, HPE has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. HPE's infringing activities relative to the '531 patent have been, and

continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

65. SPV has been damaged as a result of HPE's infringing conduct described in this Count. HPE is, thus, liable to SPV in an amount that adequately compensates SPV for HPE's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

(INFRINGEMENT OF U.S. PATENT NO. 8,270,384)

66. Plaintiff incorporates the preceding paragraphs herein by reference.

67. SPV is the assignee of the '384 patent, entitled "Wireless point that provides functions for a wireless local area network to be separated between the wireless point and one or more control nodes, and method for providing service in a wireless local area network having functions separated between a wireless point and one or more control nodes," with ownership of all substantial rights in the '384 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

68. The '384 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '384 patent issued from U.S. Patent Application No. 13/235,912.

69. HPE has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '384 patent in this judicial district and elsewhere in Texas and the United States.

70. HPE designs, develops, manufactures, assembles and markets wireless access points that are configured to establish connections with a controller and exchange information about the separation of functions between themselves and the controller.

71. HPE directly infringes the ’384 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing those Accused Products, their components and processes, and/or products containing the same that incorporate the fundamental technologies covered by the ’384 patent.

72. For example, HPE infringes claim 1 of the ’384 patent via the Accused Products, which are configured to establish connections with a controller and exchange information about the separation of functions between themselves and the controller.

73. The Accused Products comprise a “wireless point that provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes” that satisfies the limitations of claim 1. For example, the Accused Products are configured to interface with Aruba Central management platform (via Aruba Central cloud controllers, each a control node) are wireless points.

Manage any-sized network from the cloud

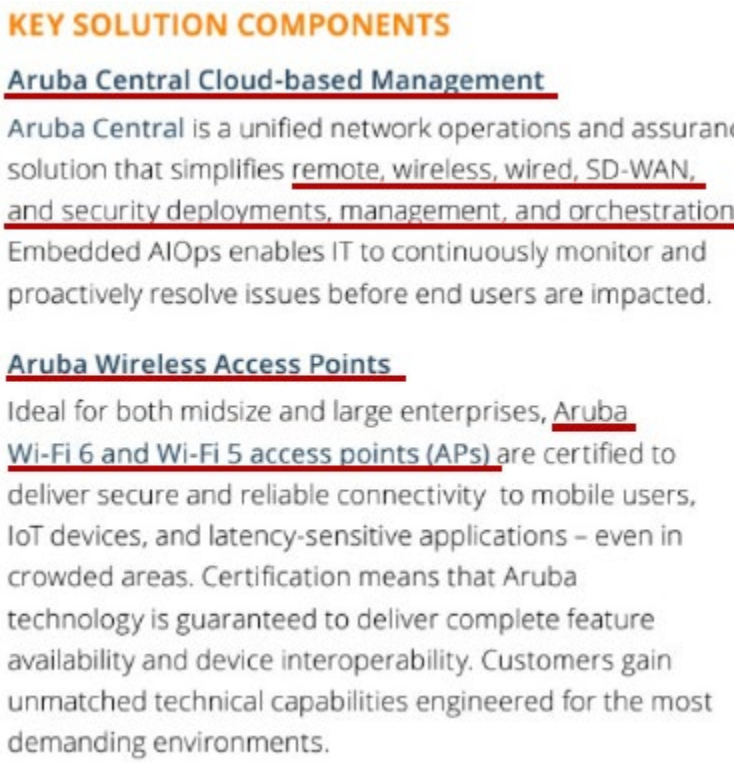
Built on a cloud-native, microservices architecture, Aruba Central is an AI-powered solution that simplifies IT operations, improves agility, and reduces costs by unifying management of all network infrastructure.

Table 1: Aruba Central Deployment Model Comparison

	Cloud (SaaS)	On-premises	Intelligent Operations for Central On-Premises
Server Appliances			
Server Options	N/A	1, 3, 5 and 7 server options	SOW based
Server Support	N/A	Optional	✓
Software			
License Model	Per device (AP, switch, gateway)	Per device (AP, switch, controller)	SOW based
License Duration	Fixed Term (1-, 3-, 5-, 7-, 10-year)	Fixed Term (1-, 3-, 5-, 7-, 10-year)	SOW based
Software Support	✓	✓	✓
Network Devices			
Scale	N/A	Up to 25K network devices	Up to 25K network devices
Supported Devices	Aruba IAPs, Switches, Gateways	Aruba APs/IAPs, Switches, Controllers, and Conductors	SOW based
Compatible OS	InstantOS, SD-WAN, AOS-S, AOS-CX	InstantOS, AOS6, AOS8, AOS-S, AOS-CX	InstantOS, AOS6, AOS8, AOS-S, AOS-CX

As used herein, an "Aruba Central WiFi system" refers to the interfacing/deployment of one or more Aruba Central-managed APs with one or more Aruba Central cloud controllers. In an Aruba

Central WiFi system one or more Aruba Central-managed APs interface with one or more Aruba Central cloud controllers (each a control node). An Aruba Central WiFi system utilizes control traffic that flows between one or more Aruba Central cloud controllers (control node) and one or more cloud-managed HPE-Aruba wireless access points (each a wireless point).



KEY SOLUTION COMPONENTS

Aruba Central Cloud-based Management

Aruba Central is a unified network operations and assuran solution that simplifies remote, wireless, wired, SD-WAN, and security deployments, management, and orchestration Embedded AIOps enables IT to continuously monitor and proactively resolve issues before end users are impacted.

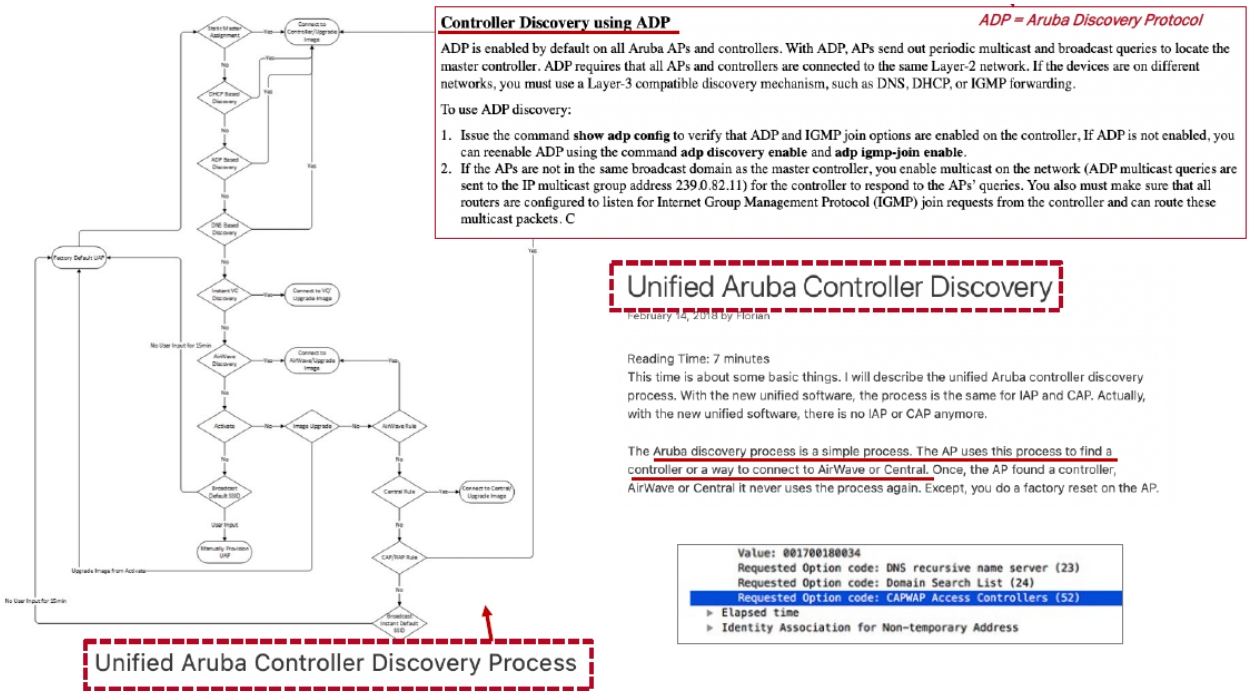
Aruba Wireless Access Points

Ideal for both midsize and large enterprises, Aruba Wi-Fi 6 and Wi-Fi 5 access points (APs) are certified to deliver secure and reliable connectivity to mobile users, IoT devices, and latency-sensitive applications – even in crowded areas. Certification means that Aruba technology is guaranteed to deliver complete feature availability and device interoperability. Customers gain unmatched technical capabilities engineered for the most demanding environments.

Aruba Central cloud controller (control node) provides network-facing functions used by the access points (e.g., provisioning and configuration). Similarly, the Aruba Central-managed APs provide separate client-facing functionality—in this way the APs provide for functions for a wireless local area network to be separated between said wireless point and one or more control nodes. Functions of an Aruba Central-managed WLAN are separated between those functions performed by the cloud controller (for example, gathering insights on all client devices connected to the network via different network components, and identifying client types and profiles) and

separate functions performed by the managed APs (for example, an AP enforces policies on a specific client, once the identity of the client is established).

74. The Accused Products comprise "a discovery unit configured to send a discovery request message to said one or more control nodes." For example, in an Aruba Central WiFi system, an Aruba Central-managed AP uses its discovery unit to send a discovery request message to an Aruba Central cloud controller (said one or more control nodes), for example, using Aruba's ADP protocol.



75. The Accused Products comprise "a selecting unit configured to select one control node of said one or more control nodes based on one or more discovery response messages sent to said wireless point from said one or more control nodes in response to said discovery request message, each of said one or more discovery response messages including information of functions offered by the associated control node of said one or more control nodes." For example, the Aruba Central-managed APs select an Aruba Central cloud controller (control node) based on a received discovery response message. For example, during the AP discovery and adoption process, the AP

selects the control node based on the control node providing an encryption key and/or otherwise being authenticated over a secure connection (including via use of TLS/X.509).

TRUSTED TRAFFIC

With the foundation of device assurance delivered by the extensive use of hardware-enforced and monitored protection, Aruba Secure Infrastructure then adds Trusted Traffic functionality to further secure the network.

Trusted Traffic starts with ArubaOS, the software architecture designed to support hardware-based network security functionality. It is built using three key components:

- A hardened, multi-threaded supervisory kernel managing administration, authentication, logging, and other system operation functions.
- An embedded real-time operating system powers the dedicated packet processing hardware of the controller, implementing all routing, switching, and Common Criteria validated firewall functions.
- A programmable, FIPS, DoDIN-APL and Common Criteria validated encryption/decryption engine built on the controller's dedicated hardware, delivering government-grade security without sacrificing performance.

Centralized encryption

Aruba's security architecture is different from all other vendors. In the default configuration, known as tunnel mode, Aruba access points (APs) do not perform encryption/decryption and thus do not contain any encryption keys. The access points receive encrypted wireless frames from the radio interface and immediately packages these encrypted wireless frames into an IP tunnel to the mobility controller. Once at the mobility controller, the IP tunnel packet header is removed and what remains is an encrypted 802.11 Wi-Fi frame. The controller then processes this frame, decrypting it and turning it back into a standard routable IP packet. Access points never have access to encryption keys, and they are unable to process the Wi-Fi traffic locally.

Public Key Authentication for SSH Access

The controller allows public key authentication of users accessing the controller using SSH. (The default is for username/password authentication.) When you import an X.509 client certificate into the controller, the certificate is converted to SSH-RSA keys. When you enable public key authentication for SSH, the controller validates the client's credentials with the imported public keys. You can specify public key authentication only, or public key authentication with username/password (if the public key authentication fails, the user can login with a configured username and password).

To use public key authentication, you must do the following:

1. Import the X.509 client certificate into the controller using the WebUI, as described in "Importing Certificates".
2. Configure SSH for client public key authentication. You can optionally also select username/password authentication.
3. Configure the username, role and client certificate.

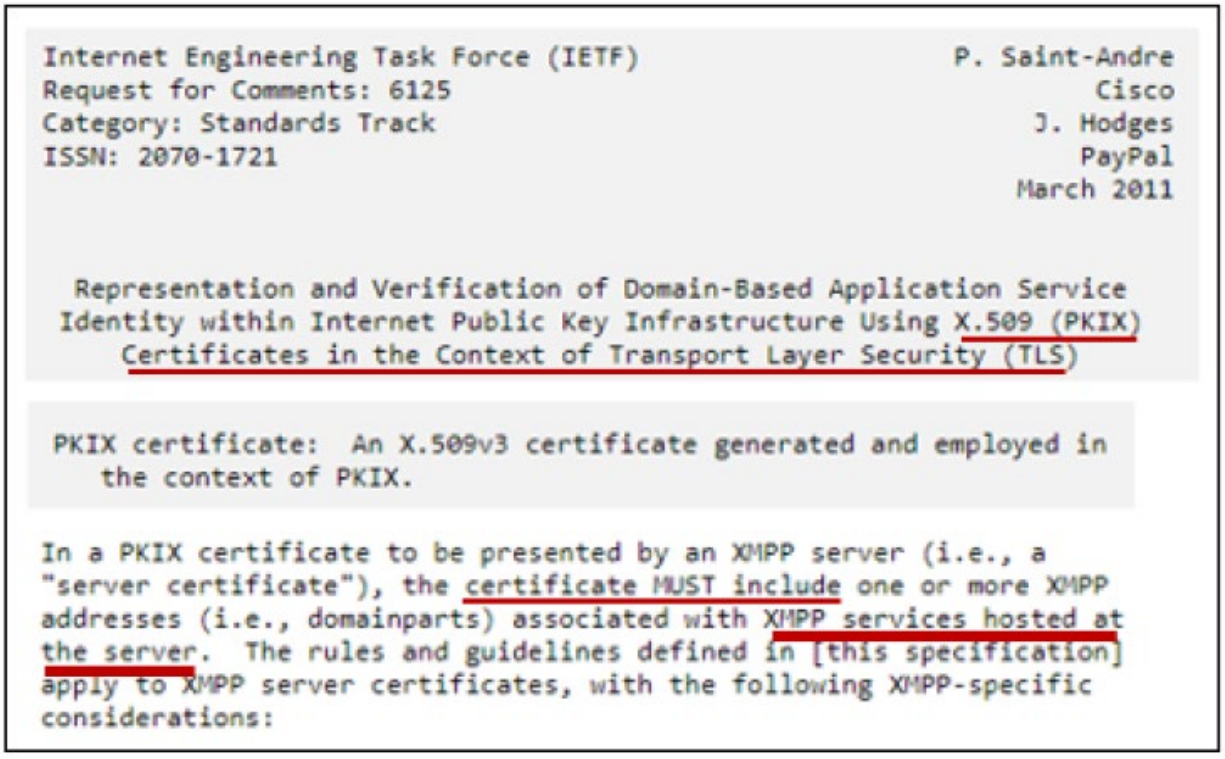
- Client certificate and client's public key. (The public key is used for applications such as SSH which does not support X509 certificates and requires the public key to verify an allowed certificate.)

Certificates can be in the following formats:

- X509 PEM unencrypted
- X509 PEM encrypted with a key

The functionality of HPE-Aruba's hardware WLAN controller products provide evidence that controller-managed HPE-Aruba APs conduct a dynamic discovery and controller selection process using an Aruba-developed discovery algorithm (e.g., ADP). The discovery response message sent

by the control node includes security related information that is used by the Aruba Central-managed AP (wireless point) during the discovery and adoption process (i.e., to "select one control node"). This security related information is dependent on the type of connection the wireless point and control node are attempting to communicate over and supported capabilities of the devices themselves for purposes of authentication. For example, on information and belief, during a L3 discovery over TLS the discovery response message includes information pertaining to a X.509 certificate of the control node, said information including service names and IDs of services offered by the control node.



Internet Engineering Task Force (IETF) P. Saint-Andre
Request for Comments: 6125 Cisco
Category: Standards Track J. Hodges
ISSN: 2070-1721 PayPal
March 2011

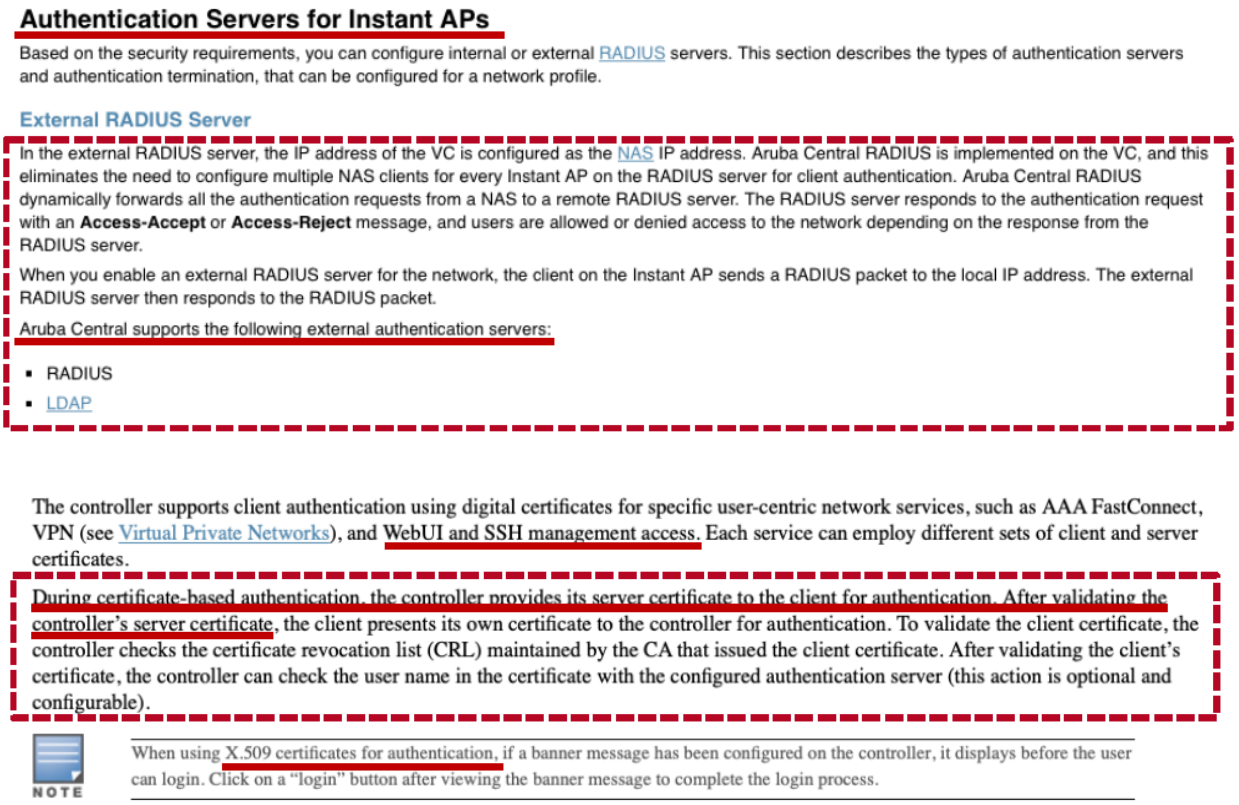
Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)

PKIX certificate: An X.509v3 certificate generated and employed in the context of PKIX.

In a PKIX certificate to be presented by an XMPP server (i.e., a "server certificate"), the certificate MUST include one or more XMPP addresses (i.e., domainparts) associated with XMPP services hosted at the server. The rules and guidelines defined in [this specification] apply to XMPP server certificates, with the following XMPP-specific considerations:

76. The Accused Products comprise "a session establishing unit configured to establish a secure session with said selected one control node." For example, as part of the discovery and adoption process the Aruba Central managed AP establishes a secure session with the chosen control node. For example, after authenticating the Aruba Central cloud controller (control node) using its X.509 certificate the AP completes establishing a secure session with the control node

over HTTPS/TLS. Aruba Central also supports external authentication means, as shown in this slide.



Authentication Servers for Instant APs

Based on the security requirements, you can configure internal or external RADIUS servers. This section describes the types of authentication servers and authentication termination, that can be configured for a network profile.

External RADIUS Server

In the external RADIUS server, the IP address of the VC is configured as the NAS IP address. Aruba Central RADIUS is implemented on the VC, and this eliminates the need to configure multiple NAS clients for every Instant AP on the RADIUS server for client authentication. Aruba Central RADIUS dynamically forwards all the authentication requests from a NAS to a remote RADIUS server. The RADIUS server responds to the authentication request with an **Access-Accept** or **Access-Reject** message, and users are allowed or denied access to the network depending on the response from the RADIUS server.

When you enable an external RADIUS server for the network, the client on the Instant AP sends a RADIUS packet to the local IP address. The external RADIUS server then responds to the RADIUS packet.

Aruba Central supports the following external authentication servers:

- RADIUS
- LDAP

The controller supports client authentication using digital certificates for specific user-centric network services, such as AAA FastConnect, VPN (see Virtual Private Networks), and WebUI and SSH management access. Each service can employ different sets of client and server certificates.

During certificate-based authentication, the controller provides its server certificate to the client for authentication. After validating the controller's server certificate, the client presents its own certificate to the controller for authentication. To validate the client certificate, the controller checks the certificate revocation list (CRL) maintained by the CA that issued the client certificate. After validating the client's certificate, the controller can check the user name in the certificate with the configured authentication server (this action is optional and configurable).

NOTE

When using X.509 certificates for authentication, if a banner message has been configured on the controller, it displays before the user can login. Click on a "login" button after viewing the banner message to complete the login process.

77. The Accused Products comprise "a negotiation unit configured to exchange information about the functions to be separated between said selected one control node and said wireless point." For example, the Aruba Central-managed AP uses its negotiation unit to exchange information about the functions to be separated between it and said selected one control node. For example, as shown below, Aruba Central's Dynamic Segmentation feature enables the control node to provide the network-facing functions used by the APs, for example identifying client types and sharing that information with the APs, while the APs separately provide client-facing functionality, for example, enforcing policies on clients once the identity of the clients are established.

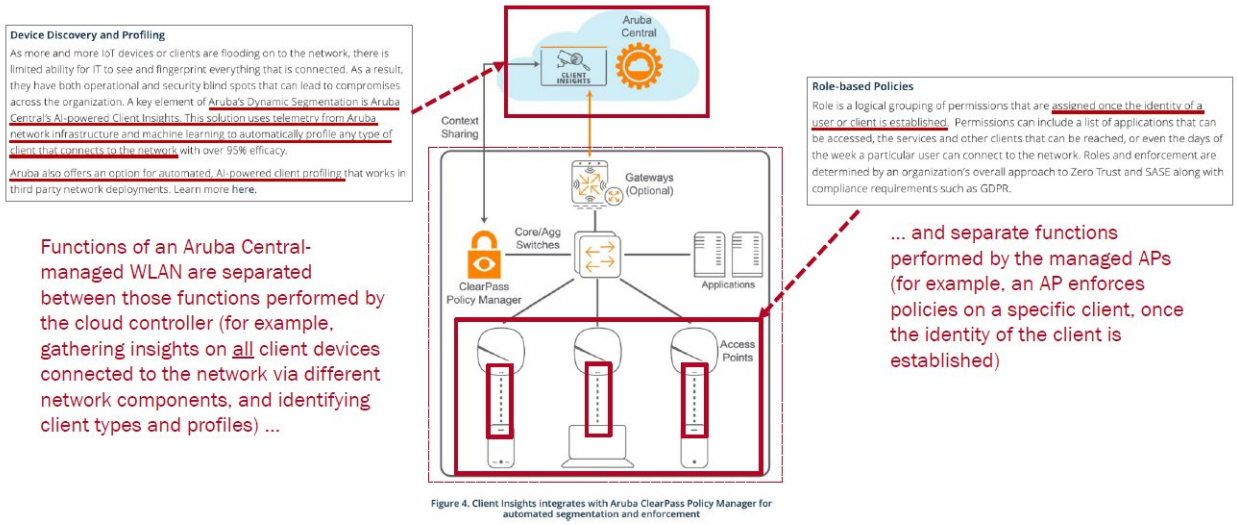


Figure 4. Client Insights integrates with Aruba ClearPass Policy Manager for automated segmentation and enforcement

78. The technology discussion above and the exemplary Accused Products provide context for Plaintiff's infringement allegations.

79. At a minimum, HPE has known of the '384 patent at least as early as the filing date of the complaint. In addition, HPE has known about the '384 patent since at least April 19, 2012, when HPE was given access to a data room providing notice of its infringement.

80. On information and belief, since at least the above-mentioned date when HPE was on notice of its infringement, HPE has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the Accused Products that include or are made using all of the limitations of one or more claims of the '384 patent to directly infringe one or more claims of the '384 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, HPE does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '384 patent. HPE intends to cause, and has taken affirmative steps to induce infringement by its distributors, importers, customers, subsidiaries, and/or consumers by at least, inter alia, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and

within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing and certifying features related to wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to these purchasers in the United States.

81. In the alternative, on information and belief, since at least the above-mentioned date when HPE was on notice of its infringement, HPE has contributorily infringed, under U.S.C. § 271(c), one or more claims of the '384 patent. For example, HPE contributes to the direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the Accused Products. To the extent that the Accused Products do not directly infringe one or more claims of the '384 patent, such products contain instructions, such as source code, that are especially adapted to cause the Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the Accused Products to exchange information about the functions to be separated between the control node and the access point in an infringing manner and are a material part of the invention of the '384 patent and are not a staple article of commerce suitable for substantial non-infringing use.

82. On information and belief, despite having knowledge of the '384 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '384 patent, HPE has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. HPE's infringing activities relative to the '384 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such

that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

83. SPV has been damaged as a result of HPE's infringing conduct described in this Count. HPE is, thus, liable to SPV in an amount that adequately compensates SPV for HPE's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IV

(INFRINGEMENT OF U.S. PATENT NO. 8,467,723)

84. Plaintiff incorporates the preceding paragraphs herein by reference.

85. SPV is the assignee of the '723 patent, entitled "Base Station Apparatus, Mobile Apparatus, and Communication Method," with ownership of all substantial rights in the '723 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

86. The '723 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '723 patent issued from U.S. Patent Application No. 13/585,621.

87. HPE has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '723 patent in this judicial district and elsewhere in Texas and the United States.

88. HPE designs, develops, manufactures, assembles and markets devices configured to connect to wireless cellular networks.

89. HPE directly infringes the '723 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing those Accused Products, their components and processes, and/or

products containing the same that incorporate the fundamental technologies covered by the '723 patent.

90. For example, HPE infringes claim 9 of the '723 patent via the Accused Products that perform inter-RAT handovers and are configured to connect wireless cellular networks.

91. The Accused Products implement the "communication method performed by a mobile station apparatus that belongs to a first area, which is covered by a base station apparatus employing a first Radio Access Technology (RAT), the first area including part or entirety of a second area which is covered by a host station employing a second RAT different from the first RAT" of claim 9. Each of the Accused Products is a mobile station that performs inter-RAT handovers, where the mobile station's radio connection is switched from a first base station (e.g., LTE eNB) that employs a first RAT (e.g., LTE) to a second base station (e.g., RNC/NodeB) that employs a second (and different) RAT (e.g., GERAN/UTRAN). RAT handover scenarios include handovers between E-UTRAN (LTE) and UTRAN or GERAN (both 3G).

92. The Accused Products transmit, to the base station apparatus, notification information while the mobile station apparatus is using the first RAT when the mobile station apparatus detects that the mobile station apparatus is located in the second area while using the first RAT. For example, the Accused Products include a transmitter (e.g., an RF transceiver coupled to a RF front end and an antenna) to transmit notification information, e.g., measurement information, to the E-UTRAN eNB (i.e., the base station) which is using a first RAT (e.g., LTE). Such a transmission occurs when the mobile station detects that it is located in a second area (i.e., within a 3G radio cell while still connected to the LTE base station).

93. The Accused Products perform a handover based on traffic control by the base station apparatus using the notification information. For example, the Accused Products have a

controller that is responsive to a handover message received from the LTE eNB, based on the notification information, i.e., the measurement information.

94. The technology discussion above and the exemplary Accused Products provide context for Plaintiff's infringement allegations.

95. At a minimum, HPE has known of the '723 patent at least as early as the filing date of the complaint. In addition, HPE has known about the '723 patent since at least April 19, 2022, when HPE was given access to a data room providing notice of its infringement. Moreover, HPE has been on notice of the '723 patent as a result of previous lawsuits filed by the Plaintiff against competitors of HPE and other relevant market participants, such as TCL, Acer, ASUS, and LG.

96. On information and belief, since at least the above-mentioned date when HPE was on notice of its infringement, HPE has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the Accused Products that include or are made using all of the limitations of one or more claims of the '723 patent to directly infringe one or more claims of the '723 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, HPE does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '723 patent. HPE intends to cause, and has taken affirmative steps to induce infringement by its distributors, importers, customers, subsidiaries, and/or consumers by at least, inter alia, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing and certifying features related to the wireless

networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to these purchasers in the United States.

97. In the alternative, on information and belief, since at least the above-mentioned date when HPE was on notice of its infringement, HPE has contributorily infringed, under U.S.C. § 271(c), one or more claims of the '723 patent. For example, HPE contributes to the direct infringement of such claims by distributors, customers, subsidiaries, importers, and/or consumers that use, import, purchase, or sell the Accused Products. To the extent that the Accused Products do not directly infringe one or more claims of the '723 patent, such products contain instructions, such as source code, that are especially adapted to cause the Accused Products to operate in an infringing manner. Such instructions are specifically designed to cause the Accused Products to perform LTE inter-RAT handovers in an infringing manner and are a material part of the invention of the '723 patent and are not a staple article of commerce suitable for substantial non-infringing use.

98. On information and belief, despite having knowledge of the '723 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '723 patent, HPE has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. HPE's infringing activities relative to the '723 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

99. SPV has been damaged as a result of HPE's infringing conduct described in this Count. HPE is, thus, liable to SPV in an amount that adequately compensates SPV for HPE's

infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

100. Plaintiff SPV is entitled to recover from HPE the damages sustained by Plaintiff as a result of HPE's wrongful acts, and willful infringement, in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

101. Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and necessary attorneys' fees, costs, and expenses.

JURY DEMAND

102. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

103. Plaintiff respectfully requests that the Court find in its favor and against HPE, and that the Court grant Plaintiff the following relief:

1. A judgment that HPE has infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;
2. A judgment for an accounting of all damages sustained by Plaintiff as a result of the acts of infringement by HPE;

3. A judgment and order requiring HPE to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
4. A judgment and order requiring HPE to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
5. A judgment and order finding this to be an exceptional case and requiring HPE to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and
6. Such other and further relief as the Court deems just and equitable.

Dated: January 10, 2023

Respectfully submitted,

/s/ *Patrick J. Conroy*
Patrick J. Conroy
Texas Bar No. 24012448
Jon Rastegar
Texas Bar No. 24064043
NELSON BUMGARDNER CONROY PC
2727 N. Harwood St.
Suite 250
Dallas, TX 75201
Tel: (817) 377-9111
pat@nelbum.com
jon@nelbum.com

John P. Murphy
Texas Bar No. 24056024
NELSON BUMGARDNER CONROY PC
3131 W 7th St
Suite 300
Fort Worth, TX 76107
Tel: (817) 806-3808
murphy@nelbum.com

ATTORNEYS FOR PLAINTIFF SOVEREIGN PEAK VENTURES, LLC