

Hewlett Packard Enterprise Company v. Sovereign Peak Ventures, LLC
Exhibit 1013
Page 000001

I. P.R. 3-1 Disclosure of Asserted Claims and Infringement Contentions

(a) Each claim of each patent in suit that is allegedly infringed by each opposing party;

By making, using, testing, offering for sale, selling, and/or importing any of the devices addressed in Exhibits A-D, Defendant directly and/or indirectly infringes 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 “patents-in-suit”). Based on information presently available, Plaintiff contends that Defendant infringes the claims identified in Exhibits A-D, including the following claims of the patents-in-suit:

1. Claim 1 of the ’512 patent;
2. Claims 1, 7, and 13 of the ’531 patent;
3. Claims 1, 3, 4, and 6 of the ’384 patent; and
4. Claims 5-7 and 9 of the ’723 patent.

(b) Separately for each asserted claim, each accused apparatus, product, device, process, method, act, or other instrumentality (“Accused Instrumentality”) of each opposing party of which the party is aware. This identification shall be as specific as possible. Each product, device, and apparatus must be identified by name or model number, if known. Each method or process must be identified by name, if known, or by any product, device, or apparatus which, when used, allegedly results in the practice of the claimed method or process;

The Accused Instrumentalities of which SPV is aware are identified below. Plaintiff reserves the right, in response to discovery or as otherwise permitted, to supplement its identification of Accused Instrumentalities.

1. The Accused Instrumentalities for each asserted claim of the ’512 patent are identified in Exhibit A hereto.

2. The Accused Instrumentalities for each asserted claim of the '531 patent are identified in Exhibit B hereto.
3. The Accused Instrumentalities for each asserted claim of the '384 patent are identified in Exhibit C hereto.
4. The Accused Instrumentalities for each asserted claim of the '723 patent are identified in Exhibit D hereto.

Plaintiff expressly reserves the right to seek leave of Court to augment and supplement these disclosures after discovery from Defendant, or as permitted under the Patent Rules. Plaintiff expects that this disclosure may be subject to amendment or supplementation to identify and accuse additional products developed or made available after the date on which these contentions are served, or of which Plaintiff was not aware at the time that these contentions were prepared. Plaintiff reserves the right to seek leave of Court to augment and supplement this disclosure after discovery from Defendant, or as permitted under the Patent Rules.

- (c) **A chart identifying specifically where each element of each asserted claim is found within each Accused Instrumentality, including for each element that such party contends is governed by 35 U.S.C. § 112(6), the identity of the structure(s), act(s), or materials(s) in the Accused Instrumentality that performs the claimed functions;**

Charts identifying where each element of the asserted claims is found within each Accused Instrumentality are included as Exhibits A-D accompanying this document. The charts are based on publicly available information currently accessible to Plaintiff. Discovery has yet to begin, and Plaintiff reserves the right to amend its list of Accused Instrumentalities or charts after discovery from Defendant, or as permitted by the Court, the Patent Rules, or the Federal Rules of Civil Procedure.

(d) Whether each element of each asserted claim is claimed to be literally present or present under the doctrine of equivalents in the Accused Instrumentality;

As the Court has not construed any claim term, it is not yet clear whether Plaintiff will rely on the doctrine of equivalents. Accordingly, Plaintiff reserves the right to amend its infringement contentions as necessary. Based on its current understanding of the claim language and publicly available information pertaining to the Accused Instrumentalities, and without notice of any claim construction or non-infringement position from Defendant, Plaintiff asserts that Defendant literally infringes each element of the asserted claims. However, any claim element not literally present in or performed by the Accused Instrumentalities is satisfied under the doctrine of equivalents because any difference between such claim element and the accused element is insubstantial. In other words, the accused element performs substantially the same function, in substantially the same way, to achieve substantially the same result.

(e) For any patent that claims priority to an earlier application, the priority date to which each asserted claim allegedly is entitled;

Each of the patents-in-suit is entitled to a priority date no later than the filing date of the earliest application to which it claims priority. To date, Plaintiff believes the patents-in-suit have the following priority dates. Plaintiff reserves the right to amend its list of priority dates as additional information becomes available, such as in response to discovery from third parties.

- The asserted claim of the '512 patent are entitled to a priority date at least as early as March 14, 2005.
- The asserted claim of the '531 patent are entitled to a priority date at least as early as March 2, 2004.
- The asserted claim of the '384 patent are entitled to a priority date at least as early as March 2, 2004.

- The asserted claims of the '723 patent are entitled to a priority date at least as early as July 19, 2007.

(f) **If a party claiming patent infringement wishes to preserve the right to reply, for any purpose, on the assertion that its own apparatus, product, device, process, method, act, or other instrumentality practices the claimed invention, the party must identify, separately for each asserted claim, each such apparatus, product, device, process, method, act, or other instrumentality that incorporates or reflects that particular claim.**

Plaintiff is not aware of any apparatus, product, device, process, method, act, or other instrumentality of its own that practices the claimed inventions.

II. P.R. 3-2 Document Production Accompanying Disclosure

(a) Plaintiff is not presently aware of any non-privileged documents sufficient to evidence discussion with, disclosure to, or other manner of providing to a third party, or sale of or offer to sell, the claimed inventions prior to the date of application for the patents-in-suit.

(b) Plaintiff is not presently aware of any non-privileged documents that evidence conception, reduction to practice, design, and development of each claimed invention that were created on or before the above referenced dates for each of the patents-in-suit. Plaintiff notes that documents responsive to P.R. 3-2(b) may be in the possession of the inventors and/or original assignees of the patents-in-suit. In the event that discovery leads to documents that evidence conception, reduction to practice, design, and development of any claimed invention that were created on or before the date of application for the patents-in-suit, Plaintiff reserves the right to claim such date.

(c) Copies of the file histories for the patents-in-suit are produced herewith and bear production numbers as follows: SPV-HPE000001 – SPV-HPE000416; SPV-HPE000459 – SPV-HPE000934; SPV-HPE000961 – SPV-HPE001272; SPV-HPE001298 – SPV-HPE001512.

Dated: February 28, 2023

Respectfully submitted,

By: /s/ Jon Rastegar

Patrick J. Conroy

Texas Bar No. 24012448

T. William Kennedy Jr.

Texas Bar No. 24055771

Jonathan H. Rastegar

Texas Bar No. 24064043

NELSON BUMGARDNER CONROY PC

2727 North Harwood St., Suite 250

Dallas, TX 75201

Tel: (214) 446-4951

pat@nbafirm.com

bill@nbafirm.com

jon@nbafirm.com

Attorneys for Plaintiff

Sovereign Peak Ventures, LLC

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document was served on Defendant through its respective counsel via e-mail on February 28, 2023.

/s/ Jon Rastegar

Ex. A - U.S. Patent No. 7,796,512

HPE makes, uses, tests, offers for sale, sells, and/or imports devices that have been or are enabled for 802.11k (the “Accused Products”). The Accused Products are identified in Appendix A to this Exhibit. Each of the Accused Products include the features identified in this chart. The features and functionality identified in this chart cause the Accused Products to practice the asserted claims of U.S. Patent No. 7,796,512 (the “’512 patent”). The Accused Products include any device that HPE makes, uses, tests, offers for sale, sells, and/or imports that have been or are enabled for 802.11k. The Accused Products include, but are not limited to, HPE-Aruba APs that are compatible with both controller-based Aruba network environment (e.g., ArubaOS) and controller-less Aruba network environment (e.g., Aruba Instant), including, but not limited to, the systems and devices listed in Appendix A.

The specific ways in which the Accused Products are enabled for 802.11k will be detailed in documents and/or source code that will be produced in discovery. SPV reserves the right to supplement this contention upon receipt of such discovery.

Appendix A is not intended to be exhaustive. HPE directly infringes the asserted claims of the ’512 patent because the Accused Products comprise or perform all elements of the asserted claims. Among other things, HPE practices the asserted method claims by testing the Accused Products. Further, the operation of the Accused Products on a network is done under the direction or control of HPE. HPE also indirectly infringes the asserted claims of the ’512 patent by encouraging its customers and end-users to deploy the Accused Products, creating advertisements that promote infringing use, maintaining distribution channels for the Accused Products, distributing or making available instructions or manuals for the Accused Products, and providing technical support, replacement parts, or services for the Accused Products.

CONFIDENTIAL

U.S. Patent No. 7,796,512

A switching source device for moving a session established with a communication counterpart to a switching destination device, comprising:	Each Accused Product is a switching source device. For example, the accused products include, but are not limited to, HPE-Aruba APs that are compatible with both controller-based Aruba network environment (e.g., ArubaOS). Each Accused Product is a switching source device that assists connected clients with roaming to a switching source destination device (destination AP). DATA SHEET ARUBAOS Enhanced network operating system for today's digital workplace Wireless • IEEE 802.11a/b/g/n/ac/ax 5 GHz, 2.4 GHz • IEEE 802.11d Additional Regulatory Domains • IEEE 802.11e QoS • IEEE 802.11h Spectrum and TX Power Extensions for 5 GHz in Europe • IEEE 802.11i MAC Security Enhancements • IEEE 802.11k Radio Resource Management • IEEE 802.11ac Enhancements for Very High Throughput • IEEE 802.11ax • IEEE 802.11n Enhancements for Higher Throughput • IEEE 802.11r Fast BSS Transition (FT) • IEEE 802.11v Wireless Network Management (partial support) • IEEE 802.11mc • IEEE 802.11w SLA-grade application assurance: ArubaOS provides complete orchestration for Air Slice, an application assurance technology unique to Aruba Wi-Fi 6 access points. By allocating radio resources, such as time, Source: https://www.arubanetworks.com/resource/arubaos-data-sheet/ Fast BSS Transition (802.11r) ArubaOS provides support for Fast BSS Transition as part of the 802.11r implementation. Fast BSS Transition mechanism minimizes the delay when a voice client transitions from one BSS to another within the same ESS. Fast BSS Transition establishes security and QoS states at the target AP before or during a re-association. This minimizes the time required to resume data connectivity when a BSS transition happens. Starting from ArubaOS 8.7.0.0, the WPA3 opmodes support fast BSS transition. Configuring Fast BSS Transition To enable and configure Fast BSS Transition on a configuration node, you must create and configure an 802.11r profile. Radio Resource (802.11k) and BSS Transition Management (802.11v) The 802.11k protocol provides mechanisms for APs and clients to dynamically measure the available radio resources. In an 802.11k enabled network, APs and clients can send neighbor reports, beacon reports, and link measurement reports to each other. This allows the APs and clients to take appropriate connection actions. The 802.11v BSS Transition capability can improve throughput, data rates and QoS for the voice clients in a network by shifting (via transition) the individual voice traffic loads to more appropriate points of association within the ESS. Configuring Radio Resource Management Information Elements ArubaOS supports the following radio resource management (RRM) information elements for APs with 802.11k support enabled. Source: https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/virtual-ap/fast-bss-tran.htm
---	--

U.S. Patent No. 7,796,512

A switching source device for moving a session established with a communication counterpart to a switching destination device, comprising:

Each Accused Product is a switching source device. For example, the accused products include, but are not limited to, HPE-Aruba APs that are compatible with controller-less Aruba network environment (e.g., Aruba Instant) that support 802.11k/r. Each Accused Product is a switching source device that assists connected clients with roaming to a switching source destination device (destination AP).

Aruba Instant 8.3.0.x

Fast Roaming	
	You can configure the following fast roaming options for the WLAN SSID: ■ Opportunistic Key Caching: You can enable Opportunistic Key Caching (OKC) when WPA-2 Enterprise and Both (WPA2 & WPA) encryption types are selected. If OKC is enabled, a cached PMK is used when the client roams to a new Instant AP. This allows faster roaming of clients without the need for a complete 802.1X authentication. ■ 802.11r: Selecting this check box enables fast BSS transition. The Fast BSS Transition mechanism minimizes the delay when a client transitions from one BSS to another within the same cluster. This option is available only when WPA-2 Enterprise and WPA-2 personal encryption keys are selected. ■ 802.11k: Selecting this check box enables 802.11k roaming on the SSID profile. The 802.11k protocol enables Instant APs and clients to dynamically measure the available radio resources. When 802.11k is enabled, Instant APs and clients send neighbor reports, beacon reports, and link measurement reports to each other.

Fast BSS Transition (802.11r Roaming)

802.11r is a roaming standard defined by IEEE. When enabled, 802.11r reduces roaming delay by pre-authenticating clients with multiple target Instant APs before a client roams to an Instant AP. With 802.11r implementation, clients pre-authenticate with multiple Instant APs in a cluster.

Radio Resource Management (802.11k)

The 802.11k standard provides mechanisms for Instant APs and clients to dynamically measure the available radio resources and enables stations to query and manage their radio resources. In an 802.11k-enabled network, Instant APs and clients can share radio and link measurement information, neighbor reports, and beacon reports with each other. This allows the WLAN network infrastructural elements and clients to assess resources and make optimal mobility decisions to ensure QoS and seamless continuity.

Discovery Logic Additional: ArubaOS and Aruba Instant inter-operability

In the previous Instant releases, access points are predefined as either controller-based Campus APs or controller-less Instant APs. Each legacy Instant AP is shipped with an Instant image that enables the Instant AP to act as its own virtual controller or to join an existing Instant cluster.

Starting with Instant 6.5.2.0, the new access points introduced in this release or following releases can run on both controller-based mode and controller-less mode. Based on the selected mode, the AP runs a corresponding image:

- Controller mode will run ArubaOS image.
- Controller-less mode will run Instant image.

Each access point is shipped with either a limited functionality manufacturing image or an Instant image. An access point with either of the limited functionality manufacturing image or the Instant image will run the full discovery logic. Based on that, it will download the ArubaOS or Instant image and convert to the corresponding mode.

Source: https://www.arubanetworks.com/techdocs/Instant_83x_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf

U.S. Patent No. 7,796,512

A switching source device for moving a session established with a communication counterpart to a switching destination device, comprising:	The Accused APs 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.’ APs that support 802.11k/r, such as the Accused APs, 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. 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. Source: IEEE Std 802.11-2016

a service discovery section for obtaining information as to whether a service can be provided from a neighboring communication device;	The Accused APs include a service discovery section for obtaining 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-NEIGHBORPRESP.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. <table border="1"> <tr> <td>B0</td> <td>B1</td> <td>B2</td> <td>B3</td> <td>B4</td> <td>B9</td> <td>B10</td> <td>B11</td> <td>B12</td> <td>B13</td> <td>B14</td> <td>B31</td> </tr> <tr> <td>AP Reachability</td> <td>Security</td> <td>Key Scope</td> <td>Capabilities</td> <td>Mobility Domain</td> <td>High Throughput</td> <td>Very High Throughput</td> <td>FTM</td> <td>Reserved</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Bits: 2</td> <td>1</td> <td>1</td> <td>6</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>1</td> <td>18</td> <td></td> </tr> </table> 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. Source: IEEE Std 802.11-2016	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	1	1	18	
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	1	1	18																											

a service discovery section for obtaining information as to whether a service can be provided from a neighboring communication device;	The Accused APs include a service discovery section for obtaining information used to compile a neighbor report. B4 B5 B6 B7 B8 B9 <table><tr><td>Spectrum Management</td><td>QoS</td><td>APSD</td><td>Radio Measurement</td><td>Delayed Block Ack</td><td>Immediate Block Ack</td></tr></table> Bits:111111 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. Source: IEEE Std 802.11-2016	Spectrum Management	QoS	APSD	Radio Measurement	Delayed Block Ack	Immediate Block Ack
Spectrum Management	QoS	APSD	Radio Measurement	Delayed Block Ack	Immediate Block Ack		

U.S. Patent No. 7,796,512

a service discovery section for obtaining information as to whether a service can be provided from a neighboring communication device;	The Accused APs include a service discovery section for obtaining information used to compile a neighbor report. 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. Source: IEEE Std 802.11-2016

a service discovery section for obtaining information as to whether a service can be provided from a neighboring communication device;

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

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

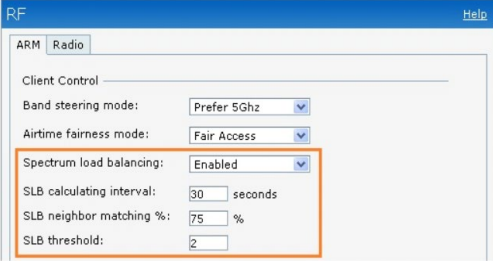
```
(host) #show lc-cluster group-membership
Cluster Enabled, Profile Name = "ap-lb"
Redundancy Mode On
```

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

Source: https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/cluster/clus-load-bala.htm?Highlight=load%20balancing

a service discovery section for obtaining information as to whether a service can be provided from a neighboring communication device;	The Accused APs' service discovery section may obtain information about neighboring communication devices from measurement reports or from background scans. For example, HPE-Aruba Instant APs ability to conduct load balancing and band steering ops among clients and other HPE-Aruba APs is evidence that these APs are aware of their RF environment via the ability to perform background scans Aruba Instant: Load balancing Dynamic Load Balancing between Two Authentication Servers You can configure two authentication servers to serve as a primary and backup RADIUS server and enable load balancing between these servers. Load balancing of authentication servers ensures that the authentication load is split across multiple authentication servers and enables the Instant APs to perform load balancing of authentication requests destined to authentication servers such as RADIUS or LDAP. The load balancing in Instant AP is performed based on outstanding authentication sessions. If there are no outstanding sessions and if the rate of authentication is low, only primary server will be used. The secondary is used only if there are outstanding authentication sessions on the primary server. With this, the load balance can be performed across RADIUS servers of asymmetric capacity without the need to obtain inputs about the server capabilities from the administrators.  Environment : This article applies to all <u>Aruba Instant Access Points running Aruba InstantOS 6.2.1.0-3.3.0.0 or higher.</u> <u>By default Spectrum Load Balancing is enabled on IAP.</u> However, follow below steps to enable: The functionality of SLB in Instant APs is controlled by three(3) configuration parameters as shown below: • SLB Calculating Interval: This interval which is mentioned in seconds determines how often spectrum load balancing must be calculated. Default: 30 seconds. Range: 100-600 • SLB Neighbor Matching: Value here indicates the percentage (%) for comparing <u>client density of IAP neighbors</u> to determine the client load on a specific AP channel. Default: 75% Range: 20% - 100% Note: Lower value in SLB Neighbor Matching triggers SLB easily and effectively. • SLB Threshold: Number here indicates the number of clients on a channel. This value is used to calculate <u>client count threshold</u>. When the load for an AP reaches or exceeds the client count threshold, load balancing is enabled on the AP. Default: 2 Range: 1-20 Note: Lower value here helps SLB to trigger easily and thereby balance the clients among IAPs in the cluster. Source: https://www.arubanetworks.com/techdocs/Instant_83x_WebHelp/Content/PDFs/Aruba%20Instant%208.3.0.x%20User%20Guide.pdf Source: https://community.arubanetworks.com/blogs/arunkumar1/2020/10/20/how-to-configure-spectrum-load-balancing-in-aruba-instant-what-are-the-parameters-and-their-default-values

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;	The Accused APs 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 <u>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</u> 9.4.2.21.7 Beacon request The Measurement Request field corresponding to a Beacon request is shown in Figure 9-156. <table><tr><td>Operating Class</td><td>Channel Number</td><td>Randomization Interval</td><td>Measurement Duration</td></tr></table> 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. Source: IEEE Std 802.11-2016	Operating Class	Channel Number	Randomization Interval	Measurement Duration
Operating Class	Channel Number	Randomization Interval	Measurement Duration		

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;	The Accused APs 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. <table><tr><td>B0</td><td>B1</td><td>B2</td><td>B3</td><td>B4</td><td>B9</td><td>B10</td><td>B11</td><td>B12</td><td>B13</td><td>B14</td><td>B31</td></tr><tr><td>AP Reachability</td><td>Security</td><td>Key Scope</td><td>Capabilities</td><td>Mobility Domain</td><td>High Throughput</td><td>Very High Throughput</td><td>FTM</td><td>Reserved</td><td></td><td></td><td></td></tr><tr><td>Bits: 2</td><td>1</td><td>1</td><td>6</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>18</td><td></td></tr></table> Figure 9-296—BSSID Information field Source: IEEE Std 802.11-2016	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	1	1	18	
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	1	1	18																											

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;	The Accused APs 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-NEIGHBORRESP.request <table><tr><th>Name</th><th>Type</th><th>Valid range</th><th>Description</th></tr><tr><td>NeighborListSet</td><td>Set of Neighbor List elements each as defined in the Neighbor Report element format</td><td>As defined in 9.4.2.37</td><td>A set of Neighbor List elements, each representing a neighboring AP being reported as defined in the Neighbor Report element format.</td></tr><tr><td>VendorSpecificInfo</td><td>A set of elements</td><td>As defined in 9.4.2.26</td><td>Zero or more elements.</td></tr></table>	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.
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.										

Source: IEEE Std 802.11-2016

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;

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.

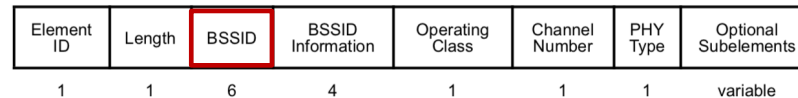


Figure 9-295—Neighbor Report element format

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.

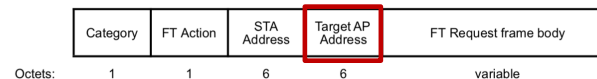


Figure 9-688—FT Request frame Action field format

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.

Source: IEEE Std 802.11-2016

U.S. Patent No. 7,796,512

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 and;	The Remote Request Broker (RRB) of an Accused AP 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 Source: IEEE Std 802.11-2016

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 and;

The Remote Request Broker (RRB) of an Accused AP establishes a session, over the DS, with the switching destination candidate device (target AP).

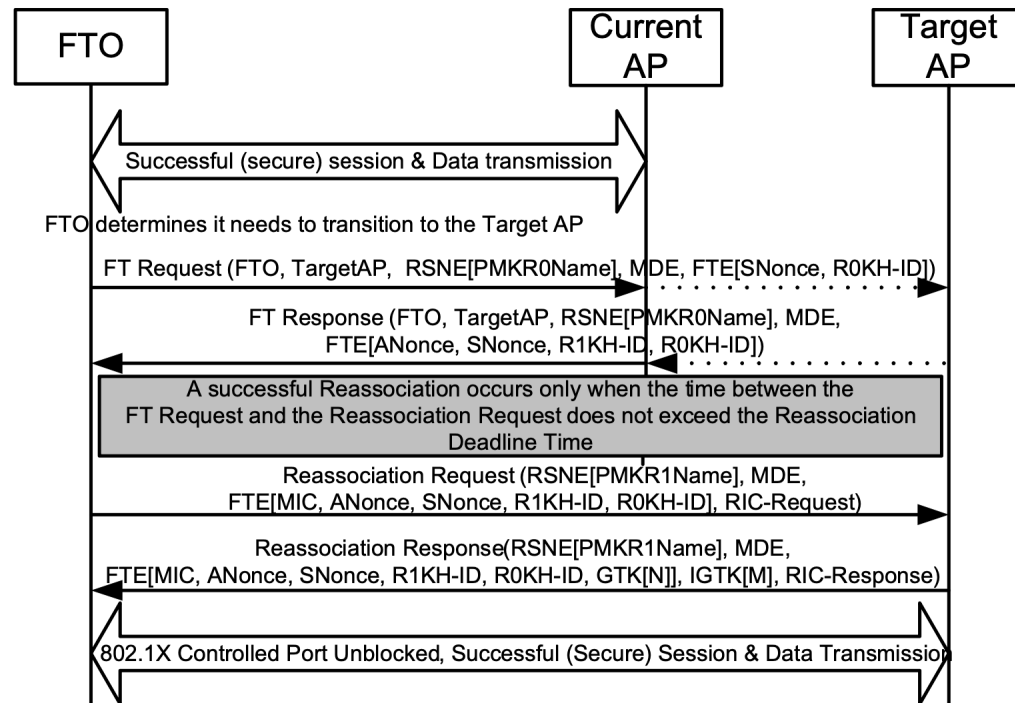


Figure 13-5—Over-the-DS FT protocol in an RSN

Source: IEEE Std 802.11-2016

U.S. Patent No. 7,796,512

an input section for receiving a switching destination candidate device list request from a user; and	The Accused APs 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 <u>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.</u> If an SSID element is Source: IEEE Std 802.11-2016

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;	The Accused APs 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. Source: IEEE Std 802.11-2016

wherein when the high speed device switching section 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.

When an Accused AP receives a switching request (FT Action Request) from a user's device, it sends a RemoteRequest to the Target AP.

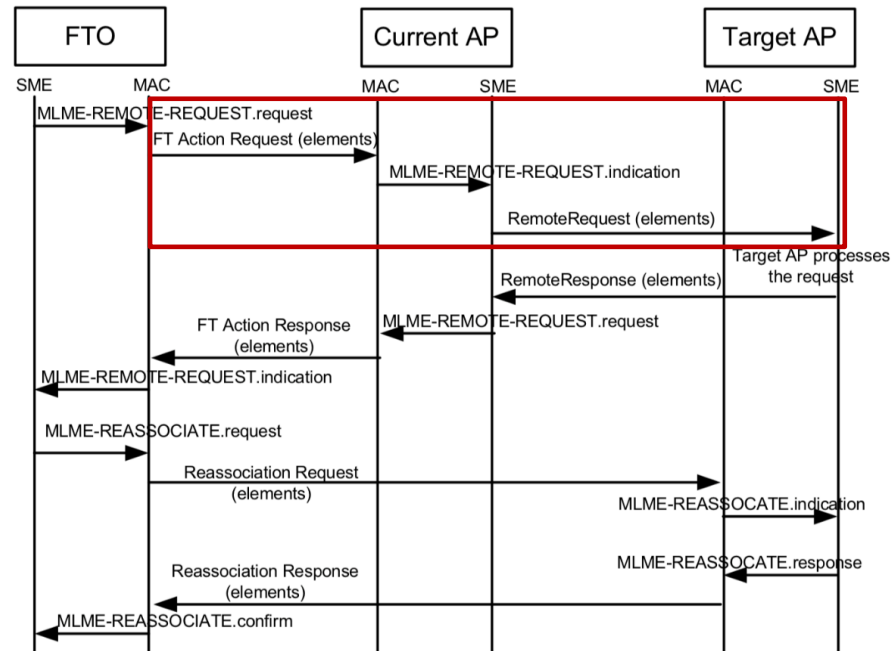


Figure 13-6—MLME interfaces for over-the-DS FT protocol messages

Source: IEEE Std 802.11-2016

wherein when the high speed device switching section 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.	The RemoteRequest 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 <i>message</i>. 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. Source: IEEE Std 802.11-2016

APPENDIX A TO EX. A

Model No.	Part No.
AP-503H	R3V38A
AP-503H	R7G97A
AP-505H	R3V48A
AP-505H	R3V57A
AP-503H	R3V39A
AP-505H	R3V49A
AP-303H	JZ088A
AP-303H	JY680A
AP-303H	JY681A
AP-203R	JY714A
AP-203R	JY715A
AP-203RP	JY722A
AP-203RP	JY723A
AP-655	R7J39A
AP-655	R7J44A
AP-635	R7J28A
AP-635	R7J33A
AP-615	R7J50A
AP-615	R7J55A
AP-555	JZ357A
AP-555	JZ367A
AP-535	JZ337A
AP-534	JZ332A
AP-535	JZ347A
AP-534	JZ342A
AP-515	Q9H63A

APPENDIX A TO EX. A

AP-514	Q9H58A
AP-515	Q9H73A
AP-514	Q9H68A
AP-505	R2H29A
AP-504	R2H23A
AP-505	R2H39A
AP-504	R2H34A
AP-344	JZ023A
AP-344	JZ024A
AP-345	JZ033A
AP-345	JZ034A
AP-303	JZ321A
AP-303P	R0G69A
AP-303P	R2H45A
AP-584	R7S99A
AP-585	R7T04A
AP-587	R7T09A
AP-584	R7T14A
AP-585	R7T19A
AP-587	R7T24A
AP-585EX	R7T29A
AP-587EX	R7T34A
AP-574	R4H13A
AP-575	R4H18A
AP-577	R4H23A
AP-574	R4H28A
AP-575	R4H33A

APPENDIX A TO EX. A

AP-577	R4H38A
AP-575EX	R4W34A
AP-577EX	R4W39A
AP-565	R4W44A
AP-567	R4W49A
AP-565	R4W54A
AP-567	R4W59A
AP-565EX	R4W63A
AP-567EX	R4W67A
AP-518	R4H03A
AP-518	R4H08A
AP-387	R0K14A
AP-387	R4E11A
AP-374	JZ163A
AP-375	JZ173A
AP-377	JZ183A
AP-374	JZ168A
AP-375	JZ178A
AP-377	JZ188A
AP-375EX	R3P69A
AP-377EX	R3P90A
AP-375ATEX	R7J11A
AP-365	JX967A
AP-365	JZ969A
AP-367	JX974A
AP-367	JX976A
AP-318	JZ153A

APPENDIX A TO EX. A

AP-318	JZ158A
--------	--------

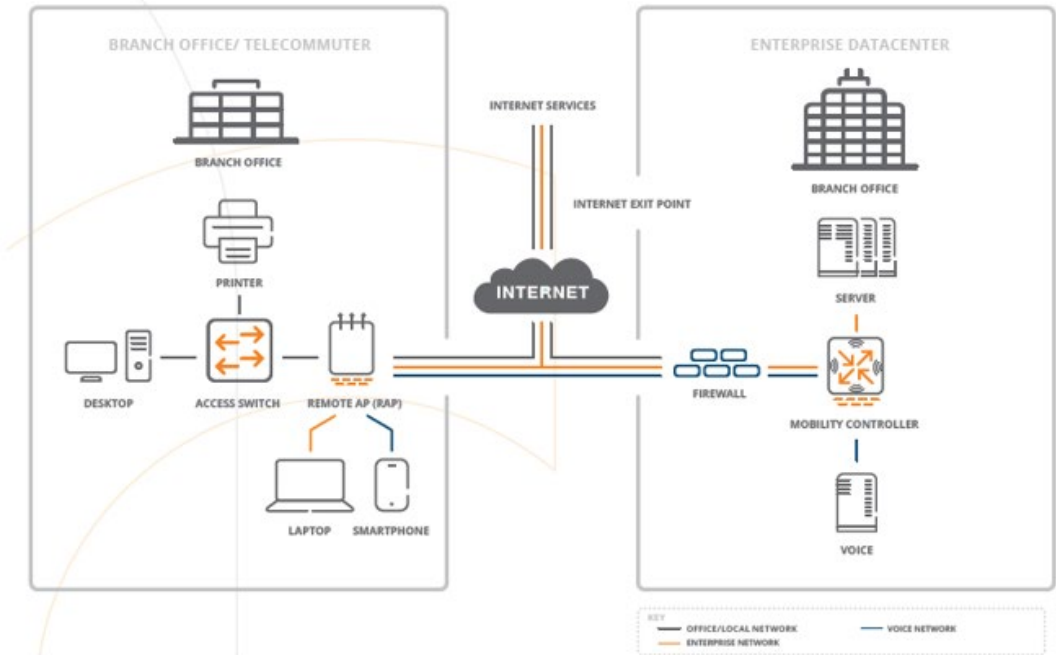
Ex. B - U.S. Patent No. 8,045,531

HPE makes, uses, tests, offers for sale, sells, and/or imports devices that support Control and Provisioning of Wireless Access Points ("CAPWAP") (the "Accused Products"). The Accused Products are identified in Appendix A to this Exhibit. Each of the Accused Products include the features identified in this chart. The features and functionality identified in this chart cause the Accused Products to practice the asserted claims of U.S. Patent No. 8,045,531 (the "'531 patent"). The Accused Products include any WLAN device that HPE makes, uses, tests, offers for sale, sells, and/or imports that supports CAPWAP. The Accused Products include, but are not limited to, HPE's ArubaOS, access points, and mobility controllers, including, but not limited to, the systems and devices listed in Appendix A.

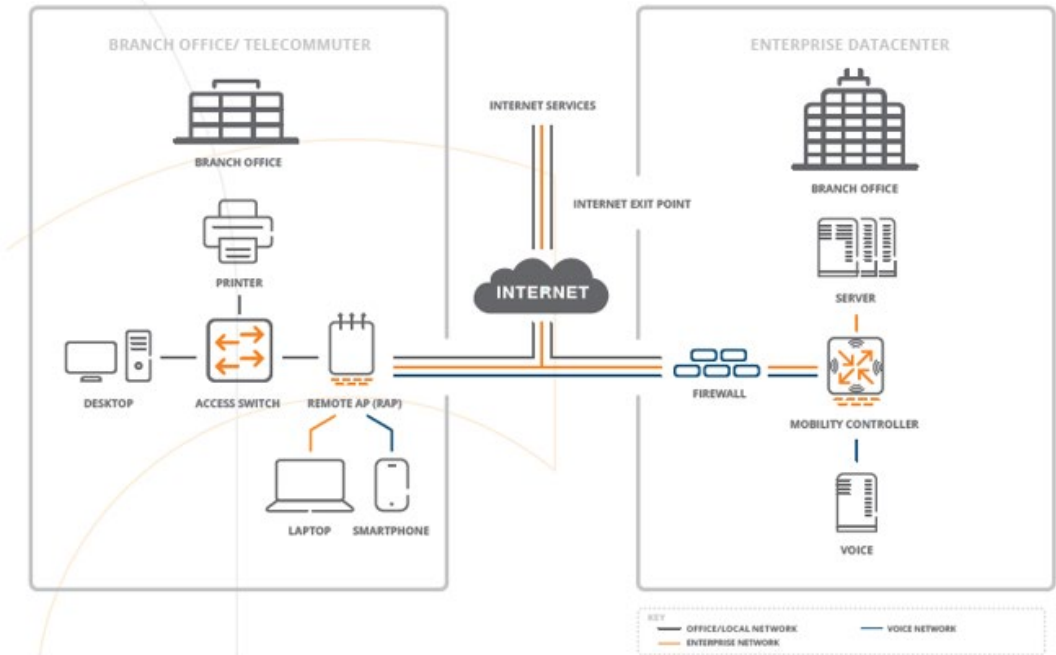
The specific ways in which the Accused Products support CAPWAP will be detailed in documents and/or source code that is produced in discovery. SPV reserves the right to supplement this contention upon receipt of such discovery.

Appendix A is not intended to be exhaustive. HPE directly infringes the asserted claims of the '531 patent because the Accused Products comprise or perform all elements of the asserted claims. Among other things, HPE practices the asserted method claims by testing the Accused Products. Further, the operation of the Accused Products on a WLAN is done under the direction or control of HPE. For example, HPE deploys the Accused Products with built-in firmware to perform CAPWAP. This firmware controls the operation of the Accused Products and cannot be altered by end users. HPE also indirectly infringes the asserted claims of the '531 patent by encouraging its customers and end-users to deploy the Accused Products in a WLAN that supports CAPWAP, creating advertisements that promote infringing use, maintaining distribution channels for the Accused Products, distributing or making available instructions or manuals for the Accused Products, and providing technical support, replacement parts, or services for the Accused Products. Moreover, the Accused Products contain instructions, such as executable firmware, that cause the device to infringe the asserted claims.

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS
A system for providing service in a wireless local area network comprising:	Each Accused Product is a system for providing service in a local area network. For example, the Accused Products include, but are not limited to HPE ArubaOS network operating system. DATA SHEET ARUBAOS <u>Enhanced network operating system for today's digital workplace</u>  Source: https://www.arubanetworks.com/assets/ds/DS_ArubaOS.pdf

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS
A system for providing service in a wireless local area network comprising:	Each Accused Product is a system for providing service in a wireless local area network. For example, the Accused Products include, but are not limited to HPE ArubaOS network operating system. DATA SHEET ARUBAOS Enhanced network operating system for today's digital workplace  Source: https://www.arubanetworks.com/assets/ds/DS_ArubaOS.pdf

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS
a single or plurality of wireless access points (WAP) for processing a subset of complete functionality defined for the wireless local area network;	The Accused Products comprise a single or a plurality of WAPs, which includes all HPE Aruba AP models that can be managed by an Aruba Mobility Controller. Source: https://www.arubanetworks.com/products/wireless/access-points/ ArubaOS 8 Topology Migration from a an ArubaOS 6 topology to an ArubaOS 8 topology primarily consists of replacing the Master controller with a Mobility Master and replacing all local and branch controllers with Mobility Controllers. Figure 12 ArubaOS 8 Topology Source: https://www.arubanetworks.com/assets/tg/TD_ArubaOS-8-Fundamental-Guide.pdf

CONFIDENTIAL

U.S. Patent No. 8,045,531

Claim 1	ACCUSED PRODUCTS
a single or plurality of wireless access points (WAP) for processing a subset of complete functionality defined for the wireless local area network;	The single or plurality of WAPs process a subset of complete functionality defined for the WLAN. The WAPs implement client-facing WLAN functions such as ClientMatch, which is an example of a subset of complete WLAN functionality. 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) Source: https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN-for-Roaming-Devices.pdf

CONFIDENTIAL

5

Claim 1	ACCUSED PRODUCTS
a single or plurality of wireless access points (WAP) for processing a subset of complete functionality defined for the wireless local area network;	The single or plurality of WAPs process a subset of complete functionality defined for the WLAN. The WAPs implement client-facing WLAN functions such as Air Slice, which is an example of a subset of complete WLAN functionality. 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, <u>at which point an Aruba AP will provide Air Slice with visibility into the user role, device type, and ongoing application use.</u> 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. Source: https://www.arubanetworks.com/assets/tg/TB_Air-Slice.pdf

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS				
a single or plurality of wireless access points (WAP) for processing a subset of complete functionality defined for the wireless local area network;	The single or plurality of WAPs process a subset of complete functionality defined for the WLAN. The WAPs implement client-facing WLAN functions such as 802.11k Radio Resource Management, which is an example of a subset of complete WLAN functionality. Configuring Radio Resource Management Information Elements <u>ArubaOS supports the following radio resource management information elements (RRM IEs) for APs with 802.11k support enabled.</u> 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 <table data-bbox="566 858 1696 1041"> <thead> <tr> <th>Parameter</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Advertise Enabled Capabilities IE</td><td>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 <u>capability is enabled</u>. A value of "Disabled" prevents the advertisement of the RRM Enabled Capabilities IE in the beacon frames when 802.11K capability is enabled.</td></tr> </tbody> </table> Source: https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VirtualAPs/Radio_Resource_Management_(802.11k).htm	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 <u>capability is enabled</u> . A value of "Disabled" prevents the advertisement of the RRM Enabled Capabilities IE in the beacon frames when 802.11K capability is enabled.
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 <u>capability is enabled</u> . A value of "Disabled" prevents the advertisement of the RRM Enabled Capabilities IE in the beacon frames when 802.11K capability is enabled.				

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS
a single or plurality of control nodes (CN) for providing a subset or complete functionalities defined for the wireless local area network; and	The Accused Products comprise a single or plurality of HPE Aruba Mobility Controllers that are control nodes. Chapter 2: Understanding the Aruba Mobility Controller Chapter 2: Understanding the <u>Aruba Mobility Controller</u> <u>The Aruba Mobility Controller is the heart of the Aruba dependent access point (AP) WLAN architecture.</u> The mobility controller is responsible for many of the operations that traditionally would be handled by an autonomous AP, and it <u>delivers additional functionality for control, security, operation, and troubleshooting.</u> 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS
a single or plurality of control nodes (CN) for providing a subset or complete functionalities defined for the wireless local area network; and	The single or plurality of Mobility Controllers process a subset of complete functionality defined for the WLAN. The Mobility Controllers implement network-facing WLAN functions such as AirMatch, which is an example of a subset of complete WLAN functionality. AirMatch in ArubaOS 8 <u>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.</u> 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: ■ <u>A centralized RF optimization service</u> ■ 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 Source: https://www.arubanetworks.com/assets/tg/TD_ArubaOS-8-Fundamental-Guide.pdf

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS
a single or plurality of control nodes (CN) for providing a subset or complete functionalities defined for the wireless local area network; and	The single or plurality of Mobility Controllers process a subset of complete functionality defined for the WLAN. The Mobility Controllers implement network-facing WLAN functions such as Web Content Classification, which is an example of a subset of complete WLAN functionality. Web Content Classification <u>Web Content Classification (WebCC)</u> is a feature on <u>Aruba controllers and IAPs</u> 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 Source: https://www.arubanetworks.com/assets/tg/TD_ArubaOS-8-Fundamental-Guide.pdf

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS
a single or plurality of control nodes (CN) for providing a subset or complete functionalities defined for the wireless local area network; and	The single or plurality of Mobility Controllers process a subset of complete functionality defined for the WLAN. The Mobility Controllers implement network-facing WLAN functions such as dynamic load balancing, which is an example of a subset of complete WLAN functionality. Leader Election In every cluster <u>one MC will be selected as the cluster leader. The cluster leader has multiple responsibilities</u> including: ■ Determining which clients are mapped to each cluster member. ■ <u>Dynamically load balancing</u> 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. Source: https://www.arubanetworks.com/assets/tg/TD_ArubaOS-8-Fundamental-Guide.pdf

Claim 1	ACCUSED PRODUCTS
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;	The Accused Products comprise a negotiation unit for the single or plurality of WAPs to negotiate with the Mobility Controller. The discovery and response signaling for the Aruba Discovery Protocol occurs via a WAP negotiation unit. 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) <u>for the Mobility Master to respond to the APs' queries</u>. 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. Source: https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/access-points/enab-ctrl-disc.htm

CONFIDENTIAL

12

Claim 1	ACCUSED PRODUCTS
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;	The Accused Products comprise a negotiation unit for the single or plurality of WAPs to negotiate with the Mobility Controller. The Mobility Controller provides certificate-based IPsec security for a secure connection. For example, TLS/X.509 certificates involve a negotiation of the parameters of the secure connection between the Mobility Controller and the WAPs. 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, <u>security</u>, 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 • <u>Providing certificate-based IPsec security to protect control channel information</u> • 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

U.S. Patent No. 8,045,531

Claim 1	ACCUSED PRODUCTS
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;	The Accused Products comprise a negotiation unit for the single or plurality of WAPs to negotiate with the Mobility Controller. The discovery and WAP/network confirmation process involves the HPE Aruba Mobility Controller and the HPE Aruba AP negotiating a functional split arrangement, where some functions are handled by the WAPs and some functions are handled by the Mobility Controller. Masters are responsible for the following functions in the WLAN: • Policy configuration: <u>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.</u> • AP white lists: <u>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.</u> • 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: <u>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.</u> • 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

14

Claim 1	ACCUSED PRODUCTS
whereby the control node 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.	The Mobility Controller negotiates with the WAPs via the negotiating unit and provides the network-facing functionalities to complement the AP's client-facing functionalities, thereby forming complete functionality defined for the WLAN according to the function split arrangement decided by the negotiating unit. 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. <u>The functionality that the mobility controller provides includes:</u> • 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. CN network-facing functionality Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

15

Claim 1	ACCUSED PRODUCTS
whereby the control node 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.	The Mobility Controller negotiates with the WAPs via the negotiating unit and provides the network-facing functionalities to complement the AP's client-facing functionalities, thereby forming complete functionality defined for the WLAN according to the function split arrangement decided by the negotiating unit. 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. <u>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:</u> • 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. <u>Aruba AP monitors the SNR of the clients associated to it and initiates a sticky move if the following conditions are met:</u> • 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)

WAP client-facing
functionality

Source:
https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN-for-Roaming-Devices.pdf

CONFIDENTIAL

16

U.S. Patent No. 8,045,531

Claim 7	ACCUSED PRODUCTS
The system according to claim 1, wherein each of the WAPs further comprises: a discovering unit for discovering an available CN within a specified domain; and	The WAPs further comprise a discovering unit for discovering available HPE Aruba Mobility Controllers. The discovering unit discovers available CNs from a DNS server, from a DHCP server, or using Aruba Discovery Protocol. Discovery of Controller An AP can discover the IP address of the controller from a DNS server, from a DHCP server, or using the Aruba Discovery Protocol. Source: https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/access-points/enab-ctrl-disc.htm

CONFIDENTIAL

17

Claim 7	ACCUSED PRODUCTS
a secure connection negotiating unit for negotiating a secure connection with a CN that may provide the complementary functionality desired by the WAP;	The WAPs further comprise a secure connection negotiating unit for negotiating a secure connection with a Mobility Controller that may provide the network-facing complementary functionality desired by the WAP. For example, TLS/X.509 certificates involve a negotiation of the parameters of the secure connection between the Mobility Controller and the WAPs. 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 <u>that traditionally would be handled by an autonomous AP, and it delivers additional functionality for control, security, operation, and troubleshooting.</u> 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 • <u>Providing certificate-based IPsec security to protect control channel information</u> • 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

18

Claim 7	ACCUSED PRODUCTS
whereby the WAP locates the CN that provides the complementary functionality with regard to defined complete wireless local area network functions with the discovering unit and establishes a secure connection with the CN that provides the complementary functionality with the secure connection negotiating unit.	The WAPs locate the CN that provides the complementary functionality that defines the complete WLAN functions with the discovering unit. 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 <u>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.</u> Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

Claim 7	ACCUSED PRODUCTS
whereby the WAP locates the CN that provides the complementary functionality with regard to defined complete wireless local area network functions with the discovering unit and establishes a secure connection with the CN that provides the complementary functionality with the secure connection negotiating unit.	The WAPs establish a secure connection with the Mobility Controller that provides the complementary functionality with the secure connection negotiating unit. For example, TLS/X.509 certificates involve a negotiation of the parameters of the secure connection between the Mobility Controller and the WAPs. 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 <u>delivers additional functionality for control, security, operation, and troubleshooting</u>. 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 • <u>Providing certificate-based IPsec security to protect control channel information</u> • 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

20

U.S. Patent No. 8,045,531

Claim 13	ACCUSED PRODUCTS
A method for providing service in a wireless local area network (WLAN) that allows a defined WLAN function split between a wireless access point (WAP) and a single or plurality of Control Nodes (CN) comprising the steps in which:	HPE practices a method for providing service in a WLAN that allows a defined WLAN function split between a WAP and a single or plurality of 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 <u>operations that traditionally would be handled by an autonomous AP, and it delivers additional functionality for control, security, operation, and troubleshooting.</u> 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

21

U.S. Patent No. 8,045,531

Claim 13	ACCUSED PRODUCTS
a subset of WAPs processes a total of a subset of functionality of the subset of WAPs defined for the WLAN;	A subset of WAPs process a total of a subset of complete functionality defined for the WLAN. The WAPs implement client-facing WLAN functions such as ClientMatch, which is an example of a subset of complete WLAN functionality. 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. <u>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:</u> • 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. <u>Aruba AP monitors the SNR of the clients associated to it and initiates a sticky move if the following conditions are met:</u> • 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) Source: https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN-for-Roaming-Devices.pdf

CONFIDENTIAL

22

Claim 13	ACCUSED PRODUCTS
a subset of WAPs processes a total of a subset of functionality of the subset of WAPs defined for the WLAN;	A subset of WAPs process a total of a subset of complete functionality defined for the WLAN. The WAPs implement client-facing WLAN functions such as Air Slice, which is an example of a subset of complete WLAN functionality. 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, <u>at which point an Aruba AP will provide Air Slice with visibility into the user role, device type, and ongoing application use.</u> 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. Source: https://www.arubanetworks.com/assets/tg/TB_Air-Slice.pdf

CONFIDENTIAL

23

Claim 13	ACCUSED PRODUCTS				
a subset of WAPs processes a total of a subset of functionality of the subset of WAPs defined for the WLAN;	A subset of WAPs process a total of a subset of complete functionality defined for the WLAN. The WAPs implement client-facing WLAN functions such as 802.11k Radio Resource Management, which is an example of a subset of complete WLAN functionality. Configuring Radio Resource Management Information Elements <u>ArubaOS supports the following radio resource management information elements (RRM IEs) for APs with 802.11k support enabled.</u> 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 <table data-bbox="566 858 1696 1041"> <thead> <tr> <th>Parameter</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Advertise Enabled Capabilities IE</td><td>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.</td></tr> </tbody> </table> Source: https://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VirtualAPs/Radio_Resource_Management_(802.11k).htm	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.
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.				

CONFIDENTIAL

Claim 13	ACCUSED PRODUCTS
the WAP dynamically negotiates with a CN for a secure connection and function split arrangement; and	The WAPs dynamically negotiate with a Mobility Controller. The Mobility Controller provides certificate-based IPsec security for a secure connection. For example, TLS/X.509 certificates involve a negotiation of the parameters of the secure connection between the Mobility Controller and the WAPs. 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, <u>security</u>, 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 • <u>Providing certificate-based IPsec security to protect control channel information</u> • 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

Claim 13	ACCUSED PRODUCTS
the WAP dynamically negotiates with a CN for a secure connection and function split arrangement; and	The WAPs dynamically negotiate with a Mobility Controller. The discovery and WAP/network confirmation process involves the HPE Aruba Mobility Controller and the HPE Aruba AP negotiating a functional split arrangement, where some functions are handled by the WAPs and some functions are handled by the Mobility Controller. 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

26

Claim 13	ACCUSED PRODUCTS
the CN provides complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision in the negotiation step.	The Mobility Controller provides the network-facing functionalities to complement the AP's client-facing functionalities, thereby forming complete functionality defined for the WLAN according to the function split arrangement decided in the negotiation step. 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. <u>The functionality that the mobility controller provides includes:</u> • 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. CN network-facing functionality Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

Claim 13	ACCUSED PRODUCTS
the CN provides complementary functionality for each of the WAPs to form a complete functionality defined for the wireless local area network according to a decision in the negotiation step.	The Mobility Controller provides the network-facing functionalities to complement the AP's client-facing functionalities, thereby forming complete functionality defined for the WLAN according to the function split arrangement decided in the negotiation step. 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. <u>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:</u> • 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. <u>Aruba AP monitors the SNR of the clients associated to it and initiates a sticky move if the following conditions are met:</u> • 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) WAP client-facing functionality Source: https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAttachments/9B71B25A-80A1-4851-8B5F-21FDC9AB083F-2-VRD_Optimizing-WLAN-for-Roaming-Devices.pdf

CONFIDENTIAL

28

APPENDIX A TO EXS. B & C

Model No.	Part No.
AP-503H	R3V38A
AP-503H	R7G97A
AP-505H	R3V48A
AP-505H	R3V57A
AP-503H	R3V39A
AP-505H	R3V49A
AP-303H	JZ088A
AP-303H	JY680A
AP-303H	JY681A
AP-203R	JY714A
AP-203R	JY715A
AP-203RP	JY722A
AP-203RP	JY723A
AP-655	R7J39A
AP-655	R7J44A
AP-635	R7J28A
AP-635	R7J33A
AP-615	R7J50A
AP-615	R7J55A
AP-555	JZ357A
AP-555	JZ367A
AP-535	JZ337A
AP-534	JZ332A
AP-535	JZ347A
AP-534	JZ342A
AP-515	Q9H63A
AP-514	Q9H58A
AP-515	Q9H73A

APPENDIX A TO EXS. B & C

AP-514	Q9H68A
AP-505	R2H29A
AP-504	R2H23A
AP-505	R2H39A
AP-504	R2H34A
AP-344	JZ023A
AP-344	JZ024A
AP-345	JZ033A
AP-345	JZ034A
AP-303	JZ321A
AP-303P	R0G69A
AP-303P	R2H45A
AP-584	R7S99A
AP-585	R7T04A
AP-587	R7T09A
AP-584	R7T14A
AP-585	R7T19A
AP-587	R7T24A
AP-585EX	R7T29A
AP-587EX	R7T34A
AP-574	R4H13A
AP-575	R4H18A
AP-577	R4H23A
AP-574	R4H28A
AP-575	R4H33A
AP-577	R4H38A
AP-575EX	R4W34A
AP-577EX	R4W39A
AP-565	R4W44A

APPENDIX A TO EXS. B & C

AP-567	R4W49A
AP-565	R4W54A
AP-567	R4W59A
AP-565EX	R4W63A
AP-567EX	R4W67A
AP-518	R4H03A
AP-518	R4H08A
AP-387	R0K14A
AP-387	R4E11A
AP-374	JZ163A
AP-375	JZ173A
AP-377	JZ183A
AP-374	JZ168A
AP-375	JZ178A
AP-377	JZ188A
AP-375EX	R3P69A
AP-377EX	R3P90A
AP-375ATEX	R7J11A
AP-365	JX967A
AP-365	JZ969A
AP-367	JX974A
AP-367	JX976A
AP-318	JZ153A
AP-318	JZ158A
9240	R7H95A
9240	R7J02
9004	R1B20A
9004	R1B25A
9012	R1B31A

APPENDIX A TO EXS. B & C

9012	R1B36A
7205	JW736A
7205	JW740A
7210	JW744A
7210DC	JW646A
7210	JW746A
7220	JW752A
7220DC	JW650A
7220	JW754A
7240XM	JW784A
7240XM	JW830A
7240XMDC	JW675A
7280	JX910A
7280	JX914A
7010	JW679A
7010	JW703A
7030	JW687A
7030	JW711A
7005	JW634A
7005	JW636A
7008	JX928A
7008	JX932A
Aruba MCR-HW-1K Mobility Conductor Hardware Appliance	JY791A
Aruba MCR-HW-5K Mobility Conductor Hardware Appliance	JY792A
Aruba MCR-HW-10K Mobility Conductor Hardware Appliance	JY793A
Aruba MCR-HW-1K-F1 Mobility Conductor Hardware Appliance FIPS/TAA	JZ396A
Aruba MCR-HW-5K-F1 Mobility Conductor Hardware Appliance FIPS/TAA	JZ397A
Aruba MCR-HW-10K-F1 Mobility Conductor Hardware Appliance FIPS/TAA	JZ398A
Aruba LIC-AP Controller per AP Capacity License E-LTU	JW472AAE

APPENDIX A TO EXS. B & C

Aruba LIC-PEF Controller Policy Enforcement Firewall per AP License E-LTU	JW473AAE
Aruba LIC-RFP Controller RFProtect per AP License E-LTU	JW474AAE
Aruba LIC-ENT Enterprise (LIC-AP LIC-PEF LIC-RFP and LIC-AW) License Bundle E-LTU	JW471AAE
Aruba LIC-ACR Controller Advanced Cryptography 1 Session License E-LTU	Q9B90AAE
Aruba Controller Web Content Classification 1 Year Subscription E-STU	JY028AAE
Aruba Controller Web Content Classification 3 Year Subscription E-STU	JY029AAE
Aruba Controller Web Content Classification 5 Year Subscription E-STU	JY030AAE
Aruba Controller Web Content Classification 7 Year Subscription E-STU	JY031AAE
Aruba Controller Web Content Classification 10 Year Subscription E-STU	JY032AAE
Aruba LIC-VIA per VIA Client License E-LTU	JZ148AAE
Aruba MC-VA-10 Virtual Mobility Controller License (US)	Q9B95AAE
Aruba MC-VA-10 Virtual Mobility Controller License (USF1)	Q9B59AAE
Aruba MC-VA-50 Virtual Mobility Controller License (US)	JY902AAE
Aruba MC-VA-50 Virtual Mobility Controller License (USF1)	JZ392AAE
Aruba MC-VA-250 Virtual Mobility Controller License (US)	JY903AAE
Aruba MC-VA-250 Virtual Mobility Controller License (USF1)	JZ393AAE
Aruba MC-VA-1K Virtual Mobility Controller License (US)	JY904AAE
Aruba MC-VA-1K Virtual Mobility Controller License (USF1)	JZ394AAE

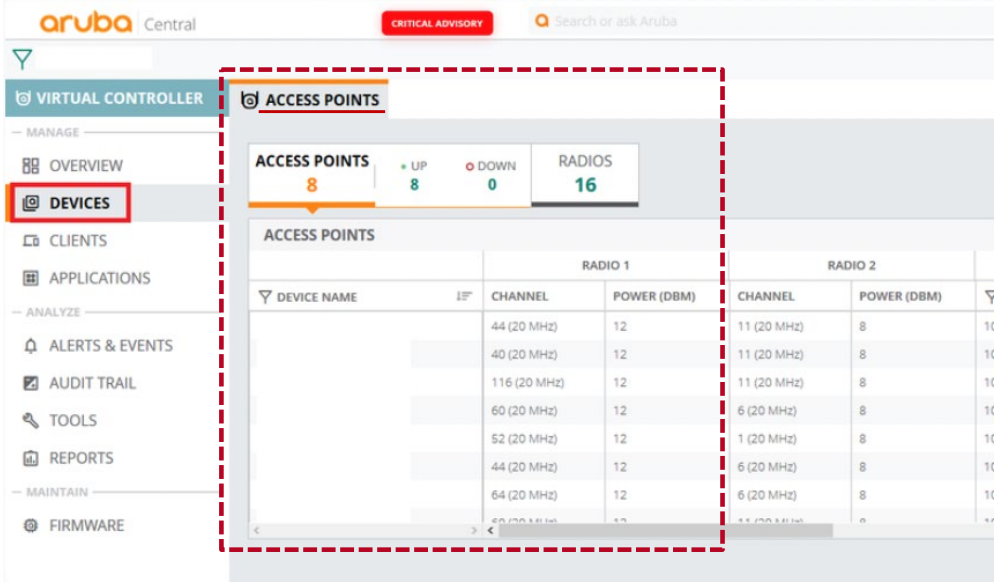
Ex. C - U.S. Patent No. 8,270,384

HPE makes, uses, tests, offers for sale, sells, and/or imports devices that support Control and Provisioning of Wireless Access Points ("CAPWAP") (the "Accused Products"). The Accused Products are identified in Appendix A to this Exhibit. Each of the Accused Products include the features identified in this chart. The features and functionality identified in this chart cause the Accused Products to practice the asserted claims of U.S. Patent No. 8,270,384 (the "'384 patent"). The Accused Products include any WLAN device that HPE makes, uses, tests, offers for sale, sells, and/or imports that supports CAPWAP. The Accused Products include, but are not limited to, HPE's ArubaOS, Aruba Central Cloud-based Management, access points, switches, and gateways, including, but not limited to, the devices listed in Appendix A.

The specific ways in which the Accused Products support CAPWAP will be detailed in documents and/or source code that is produced in discovery. SPV reserves the right to supplement this contention upon receipt of such discovery.

Appendix A is not intended to be exhaustive. HPE directly infringes the asserted claims of the '384 patent because the Accused Products comprise or perform all elements of the asserted claims. Among other things, HPE practices the asserted method claims by testing the Accused Products. Further, the operation of the Accused Products on a WLAN is done under the direction or control of HPE. For example, HPE deploys the Accused Products with built-in firmware to perform CAPWAP. This firmware controls the operation of the Accused Products and cannot be altered by end users. HPE also indirectly infringes the asserted claims of the '384 patent by encouraging its customers and end-users to deploy the Accused Products in a WLAN that supports CAPWAP, creating advertisements that promote infringing use, maintaining distribution channels for the Accused Products, distributing or making available instructions or manuals for the Accused Products, and providing technical support, replacement parts, or services for the Accused Products. Moreover, the Accused Products contain instructions, such as executable firmware, that cause the device to infringe the asserted claims.

CONFIDENTIAL

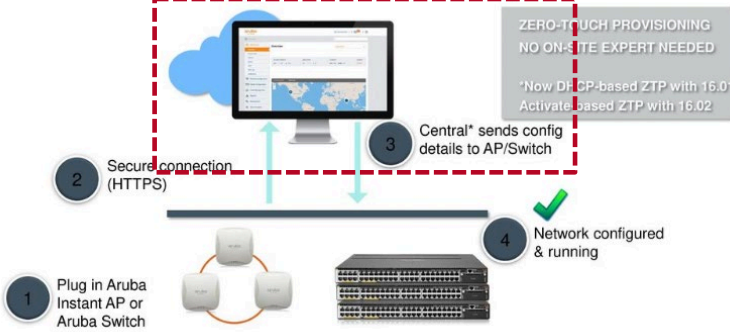
Claim 1	ACCUSED PRODUCTS
A wireless point that provides for functions for a wireless local area network to be separated between said wireless point and one or more control nodes, said wireless point comprising:	Each Accused Product is a wireless point.  Source: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=32144

U.S. Patent No. 8,270,384

Claim 1	ACCUSED PRODUCTS																																																
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, said wireless point comprising:	Each Accused Product is a wireless point. Supported Network Devices <u>Aruba Central provides management for a wide range of Aruba wireless APs, switches, and gateways (formerly known as controllers).</u> For wireless networks, Aruba Central supports deployments both with and without gateways. Review the full list of supported devices here. Table 1: Aruba Central Deployment Model Comparison <table><tr><th></th><th><u>Cloud (SaaS)</u></th><th><u>On-premises</u></th><th>Intelligent Operations for Central On-Premises</th></tr><tr><td colspan="4">Server Appliances</td></tr><tr><td>Server Options</td><td>N/A</td><td>1, 3, 5 and 7 server options</td><td>SOW based</td></tr><tr><td>Server Support</td><td>N/A</td><td>Optional</td><td>✓</td></tr><tr><td colspan="4">Software</td></tr><tr><td>License Model</td><td>Per device (AP, switch, gateway)</td><td>Per device (AP, switch, controller)</td><td>SOW based</td></tr><tr><td>License Duration</td><td>Fixed Term (1-, 3-, 5-, 7-, 10-year)</td><td>Fixed Term (1-, 3-, 5-, 7-, 10-year)</td><td>SOW based</td></tr><tr><td>Software Support</td><td>✓</td><td>✓</td><td>✓</td></tr><tr><td colspan="4">Network Devices</td></tr><tr><td>Scale</td><td>N/A</td><td>Up to 25K network devices</td><td>Up to 25K network devices</td></tr><tr><td>Supported Devices</td><td>Aruba IAPs, Switches, Gateways</td><td>Aruba APs/IAPs, Switches, Controllers, and Conductors</td><td>SOW based</td></tr><tr><td>Compatible OS</td><td>InstantOS, SD-WAN, AOS-S, AOS-CX</td><td>InstantOS, AOS6, AOS8, AOS-S, AOS-CX</td><td>InstantOS, AOS6, AOS8, AOS-S, AOS-CX</td></tr></table> Source: https://www.arubanetworks.com/assets/ds/DS_ArubaCentral.pdf		<u>Cloud (SaaS)</u>	<u>On-premises</u>	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
	<u>Cloud (SaaS)</u>	<u>On-premises</u>	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																																														

CONFIDENTIAL

3

Claim 1	ACCUSED PRODUCTS
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, said wireless point comprising:	WLAN functions are separated between said wireless point and one or more control nodes, such as Aruba Central. Manage any-sized network from the cloud Built on a cloud-native, microservices architecture, <u>Aruba Central</u> is an AI-powered solution that simplifies IT operations, improves agility, and reduces costs by unifying management of all network infrastructure. Source: https://www.arubanetworks.com/products/network-management-operations/central/ Cloud-based management with Aruba Central, and zero-touch  Source: https://slideplayer.com/slide/13652141/ (Slide: 15)

CONFIDENTIAL

Claim 1	ACCUSED PRODUCTS
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, said wireless point comprising:	The Accused Products provide client-facing functionality for the WLAN that are separated between the wireless point (AP) and one or more control nodes, such as Aruba Central. 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). Device Discovery and Profiling As more and more IoT devices or clients are flooding on to the network, there is limited ability for IT to see and fingerprint everything that is connected. As a result, they have both operational and security blind spots that can lead to compromises across the organization. A key element of Aruba's Dynamic Segmentation is Aruba Central's AI-powered Client Insights. This solution uses telemetry from Aruba network infrastructure and machine learning to automatically profile any type of client that connects to the network with over 95% efficacy. Aruba also offers an option for automated, AI-powered client profiling that works in third party network deployments. Learn more here. Source: https://www.arubanetworks.com/assets/so/SO_Dynamic-Segmentation.pdf Role-based Policies Role is a logical grouping of permissions that are assigned once the identity of a user or client is established. Permissions can include a list of applications that can be accessed, the services and other clients that can be reached, or even the days of the week a particular user can connect to the network. Roles and enforcement are determined by an organization's overall approach to Zero Trust and SASE along with compliance requirements such as GDPR. Source: https://www.arubanetworks.com/assets/so/SO_Dynamic-Segmentation.pdf Figure 4. Client Insights integrates with Aruba ClearPass Policy Manager for automated segmentation and enforcement Source: https://www.arubanetworks.com/assets/so/SO_Client-Insights.pdf

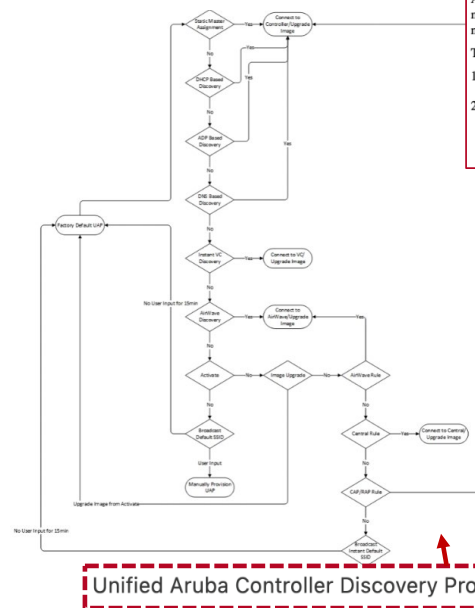
CONFIDENTIAL

Claim 1

a discovery unit configured to send a discovery request message to said one or more control nodes;

ACCUSED PRODUCTS

In an Aruba Central WiFi system, an Accused Product such as an Aruba Central-managed AP uses its discovery unit to send a discovery request message to an Aruba Central cloud controller, for example, using HPE's Aruba Discovery Protocol (ADP).



Unified Aruba Controller Discovery Process

Source: <https://www.flomain.de/2018/02/unified-aruba-controller-discovery/>

Controller Discovery using ADP

ADP is enabled by default on all Aruba APs and controllers. With ADP, APs send out periodic multicast and broadcast queries to locate the master controller. ADP requires that all APs and controllers 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. Issue the command `show adp config` to verify that ADP and IGMP join options are enabled on the controller. If ADP is not enabled, you can reenale 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 master controller, you enable multicast on the network (ADP multicast queries are sent to the IP multicast group address 239.0.82.11) for the controller to respond to the APs' queries. You also must make sure that all routers are configured to listen for Internet Group Management Protocol (IGMP) join requests from the controller and can route these multicast packets. C

Source: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/AP_Config/AP_discovery_ADP.htm

Unified Aruba Controller Discovery

FEBRUARY 14, 2018 by Florian

Reading Time: 7 minutes

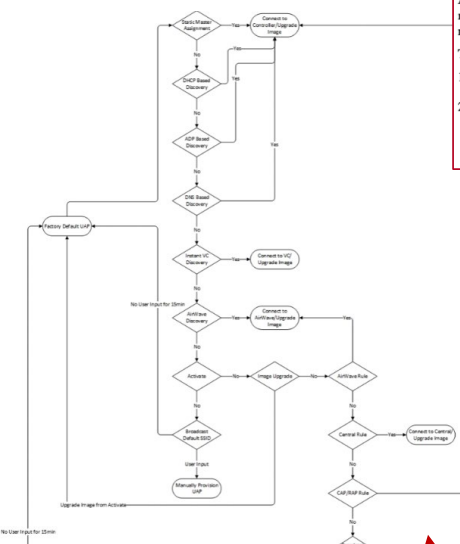
This time is about some basic things. I will describe the unified Aruba controller discovery process. With the new unified software, the process is the same for IAP and CAP. Actually, with the new unified software, there is no IAP or CAP anymore.

The Aruba discovery process is a simple process. The AP uses this process to find a controller or a way to connect to AirWave or Central. Once, the AP found a controller, AirWave or Central it never uses the process again. Except, you do a factory reset on the AP.

Value: 001700180034
Requested Option code: DNS recursive name server (23)
Requested Option code: Domain Search List (24)
Requested Option code: CAPMAP Access Controllers (52)
Elapsed time
Identity Association for Non-temporary Address

CONFIDENTIAL

6

Claim 1	ACCUSED PRODUCTS
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;	The Accused Products conduct dynamic discovery and controller selection using HPE's Aruba Discovery Protocol (ADP). Controller Discovery using ADP ADP is enabled by default on all Aruba APs and controllers. With ADP, APs send out periodic multicast and broadcast queries to locate the master controller. ADP requires that all APs and controllers 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. Issue the command <code>show adp config</code> to verify that ADP and IGMP join options are enabled on the controller. If ADP is not enabled, you can reenable ADP using the command <code>adp discovery enable</code> and <code>adp igmp-join enable</code>. 2. If the APs are not in the same broadcast domain as the master controller, you enable multicast on the network (ADP multicast queries are sent to the IP multicast group address 239.0.82.11) for the controller to respond to the APs' queries. You also must make sure that all routers are configured to listen for Internet Group Management Protocol (IGMP) join requests from the controller and can route these multicast packets. C Source: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/AP_Config/AP_discovery_ADAP.htm Unified Aruba Controller Discovery February 14, 2018 by Florian Reading Time: 7 minutes This time is about some basic things. I will describe the unified Aruba controller discovery process. With the new unified software, the process is the same for IAP and CAP. Actually, with the new unified software, there is no IAP or CAP anymore. The <u>Aruba discovery process is a simple process. The AP uses this process to find a controller or a way to connect to AirWave or Central. Once, the AP found a controller, AirWave or Central it never uses the process again. Except, you do a factory reset on the AP.</u>  Unified Aruba Controller Discovery Process Source: https://www.flomain.de/2018/02/unified-aruba-controller-discovery/ Value: 001700100034 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) Requested Option code: CAPMAP Access Controllers (52) ► Elapsed time ► Identity Association for Non-temporary Address

Claim 1	ACCUSED PRODUCTS
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;	The Accused Products conduct dynamic discovery and controller selection using HPE's Aruba Discovery Protocol (ADP). Enable Controller Discovery An AP can discover the IP address of the controller from a DNS server, from a DHCP server, or using the Aruba Discovery Protocol (ADP). <u>At boot time, the AP builds a list of controller IP addresses and then tries these addresses in order until it successfully reaches a controller.</u> This list of IP addresses provides an enhanced redundancy scheme for controllers that are located in multiple data centers separated across Layer-3 networks. The AP constructs its list of controller addresses as follows: • If the master provisioning parameter is set to a DNS name, that name is resolved and all resulting addresses are put on the list. If master is set to an IP address, that address is put on the list. • If the master provisioning parameter is not set and a controller address was received in DHCP Option 43, that address is put on the list. • If the master provisioning parameter is not set and no address was received via DHCP option 43, ADP is used to discover a controller address and that address is put on the list. • Controller addresses derived from the server-name and server-ip provisioning parameters and the default controller name aruba-master are added to the list. Note that if a DNS name resolves to multiple addresses, all addresses are added to the list. Controller Discovery using DNS When using DNS, AP learns multiple IP addresses to associate with a controller. If the primary controller is unavailable or does not respond, the AP continues through the list of learned IP addresses until it establishes a connection with an available controller. This takes approximately 3.5 minutes per controller.  It is recommended you use a DNS server to provide APs with the IP address of the master controller 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 master controller. For the DNS server to resolve this host name to the IP address of the master controller, you must configure an entry on the DNS server for the name aruba-master. Controller Discovery using ADP <u>ADP is enabled by default on all Aruba APs and controllers.</u> With ADP, APs send out periodic multicast and broadcast queries to locate the master controller. ADP requires that all APs and controllers 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. Issue the command show adp config to verify that ADP and IGMP join options are enabled on the controller. If ADP is not enabled, you can reenab 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 master controller, you enable multicast on the network (ADP multicast queries are sent to the IP multicast group address 239.0.0.2.11) <u>for the controller to respond to the APs' queries. You also must make sure that all routers are configured to listen for Internet Group Management Protocol (IGMP) join requests from the controller and can route these multicast packets.</u> C Controller discovery using a DHCP Server You can configure a DHCP server to provide the master controller's IP address. You must configure the DHCP server to send the controller'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 controller'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 controller 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 <u>"DHCP with Vendor-Specific Options" on page 1</u> or refer to the documentation included with your server. Source: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/AP_Config/AP_discovery_ADp.htm

CONFIDENTIAL

8

Claim 1	ACCUSED PRODUCTS
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;	The Accused Products, including the HPE Aruba Central-managed APs, select an Aruba Central cloud controller (i.e., 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 Mobility Master responding to the AP's queries. 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) <u>for the Mobility Master to respond to the APs' queries</u>. 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. Source: https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/access-points/enab-ctrl-disc.htm

CONFIDENTIAL

9

Claim 1	ACCUSED PRODUCTS
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;	The discovery response message sent by the control node includes security related information that is used by the wireless point during the discovery and adoption process. The security related information is dependent on the type of connection over which the wireless point and control node are attempting to communicate and dependent on the supported capabilities of the devices themselves for purposes of authentication. For example, 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. Source: https://www.rfc-editor.org/rfc/rfc6125.txt

CONFIDENTIAL

10

U.S. Patent No. 8,270,384

Claim 1	ACCUSED PRODUCTS
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;	The discovery response message sent by the control node (e.g., Mobility Master) includes policy configuration information and allows the HPE Aruba Mobility Controller and the HPE Aruba AP to negotiate a functional split arrangement, where the control node communicates its functionality to the AP. 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. <u>The policy is pushed to all locals in the form of profiles, and profiles combine to create the configuration for the dependent APs.</u> • 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: <u>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.</u> • 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

11

Claim 1	ACCUSED PRODUCTS
a session establishing unit configured to establish a secure session with said selected one control node; and	As part of the discovery and adaptation process, the Accused Product wireless point managed by HPE Aruba Central 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. <u>Authentication Servers for Instant APs</u> 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. <u>External RADIUS Server</u> 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. <u>Aruba Central supports the following external authentication servers:</u> ▪ RADIUS ▪ LDAP Source: https://help.central.arubanetworks.com/2.5.3/documentation/online_help/content/access-points/cfg/security/auth_servers.htm 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. <u>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).</u>  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. Source: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/Management_Uutilities/Managing_Certificates.htm

CONFIDENTIAL

12

Claim 1	ACCUSED PRODUCTS
a negotiation unit configured to exchange information about the functions to be separated between said selected one control node and said wireless point.	The Accused Products provide client-facing functionality for the WLAN that are separated between the wireless point (AP) and one or more control nodes, such as Aruba Central. 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). Device Discovery and Profiling As more and more IoT devices or clients are flooding on to the network, there is limited ability for IT to see and fingerprint everything that is connected. As a result, they have both operational and security blind spots that can lead to compromises across the organization. A key element of Aruba's Dynamic Segmentation is Aruba Central's AI-powered Client Insights. This solution uses telemetry from Aruba network infrastructure and machine learning to automatically profile any type of client that connects to the network with over 95% efficacy. Aruba also offers an option for automated, AI-powered client profiling that works in third party network deployments. Learn more here. Source: https://www.arubanetworks.com/assets/so/SO_Dynamic-Segmentation.pdf Role-based Policies Role is a logical grouping of permissions that are assigned once the identity of a user or client is established. Permissions can include a list of applications that can be accessed, the services and other clients that can be reached, or even the days of the week a particular user can connect to the network. Roles and enforcement are determined by an organization's overall approach to Zero Trust and SASE along with compliance requirements such as GDPR. Source: https://www.arubanetworks.com/assets/so/SO_Dynamic-Segmentation.pdf Figure 4. Client Insights integrates with Aruba ClearPass Policy Manager for automated segmentation and enforcement Source: https://www.arubanetworks.com/assets/so/SO_Client-Insights.pdf

CONFIDENTIAL

U.S. Patent No. 8,270,384

Claim 1	ACCUSED PRODUCTS
a negotiation unit configured to exchange information about the functions to be separated between said selected one control node and said wireless point.	The Accused Products provide client-facing functionality for the WLAN that are separated between the wireless point (AP) and one or more control nodes, such as Aruba Central. 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). 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

14

U.S. Patent No. 8,270,384

Claim 3	ACCUSED PRODUCTS
The wireless point according to claim 1, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.	The WLAN functions of claim 1 comprise, at least, Authentication. TRUSTED TRAFFIC With the foundation of device assurance delivered by the extensive use of hardware-enforced and monitored protection, <u>Aruba Secure Infrastructure then adds Trusted Traffic functionality to further secure the network.</u> 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. <u>Centralized encryption</u> 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. <u>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.</u> 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. Source: https://www.arubanetworks.com/assets/so/SO_SecureInfrastructure.pdf

CONFIDENTIAL

15

U.S. Patent No. 8,270,384

Claim 3	ACCUSED PRODUCTS
The wireless point according to claim 1, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.	The WLAN functions of claim 1 comprise, at least, Authentication. Source: https://www.rfc-editor.org/rfc/rfc6125.txt

CONFIDENTIAL

16

Claim 3	ACCUSED PRODUCTS
The wireless point according to claim 1, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.	The WLAN functions of claim 1 comprise, at least, Authentication. 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. <u>Aruba Central supports the following external authentication servers:</u> ▪ RADIUS ▪ LDAP Source: https://help.central.arubanetworks.com/2.5.3/documentation/online_help/content/access-points/cfg/security/auth_servers.htm 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. <u>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).</u>  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. Source: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/Management_Uilities/Managing_Certificates.htm

CONFIDENTIAL

17

Claim 4	ACCUSED PRODUCTS
A method for providing service in a wireless local area network that provides for functions for said wireless local area network to be separated between a wireless point and one or more control nodes, said method comprising:	The Accused Products practice a method for providing service in a WLAN that provides for functions in the WLAN to be separated between a wireless point (i.e., WAP or AP) and one or more control nodes (i.e., Mobility Controller or Aruba Central). Device Discovery and Profiling As more and more IoT devices or clients are flooding on to the network, there is limited ability for IT to see and fingerprint everything that is connected. As a result, they have both operational and security blind spots that can lead to compromises across the organization. A key element of Aruba's Dynamic Segmentation is Aruba Central's AI-powered Client Insights. This solution uses telemetry from Aruba network infrastructure and machine learning to automatically profile any type of client that connects to the network with over 95% efficacy. Aruba also offers an option for automated, AI-powered client profiling that works in third party network deployments. Learn more here. Source: https://www.arubanetworks.com/assets/so/SO_Dynamic-Segmentation.pdf Role-based Policies Role is a logical grouping of permissions that are assigned once the identity of a user or client is established. Permissions can include a list of applications that can be accessed, the services and other clients that can be reached, or even the days of the week a particular user can connect to the network. Roles and enforcement are determined by an organization's overall approach to Zero Trust and SASE along with compliance requirements such as GDPR. The diagram illustrates the integration of Aruba Central's Client Insights with Aruba ClearPass Policy Manager. At the top, a cloud labeled 'Aruba Central' contains a box for 'CLIENT INSIGHTS'. Below this, a dashed red box represents the network infrastructure, including 'Core/Agg Switches', 'Gateways (Optional)', 'Applications', and 'Access Points'. A 'ClearPass Policy Manager' (represented by a padlock icon) is connected to the Core/Agg Switches and the Access Points. Arrows indicate 'Context Sharing' between the Client Insights cloud and the ClearPass Policy Manager. The Access Points are shown at the bottom, connected to the network infrastructure. Figure 4. Client Insights integrates with Aruba ClearPass Policy Manager for automated segmentation and enforcement Source: https://www.arubanetworks.com/assets/so/SO_Client-Insights.pdf

CONFIDENTIAL

Claim 4	ACCUSED PRODUCTS
sending a discovery request message to said one or more control nodes;	The Accused Products send discovery request messages to control nodes as multicast and broadcast queries seeking a master controller location. Controller Discovery using ADP ADP is enabled by default on all Aruba APs and controllers. With ADP, APs send out periodic multicast and broadcast queries to locate the master controller. ADP requires that all APs and controllers 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. Issue the command <code>show adp config</code> to verify that ADP and IGMP join options are enabled on the controller. If ADP is not enabled, you can reenale ADP using the command <code>adp discovery enable</code> and <code>adp igmp-join enable</code>. 2. If the APs are not in the same broadcast domain as the master controller, you enable multicast on the network (ADP multicast queries are sent to the IP multicast group address 239.0.82.11) for the controller to respond to the APs' queries. You also must make sure that all routers are configured to listen for Internet Group Management Protocol (IGMP) join requests from the controller and can route these multicast packets. C Source: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/AP_Config/AP_discovery_ADP.htm Unified Aruba Controller Discovery FEBRUARY 14, 2018 by Florian Reading Time: 7 minutes This time is about some basic things. I will describe the unified Aruba controller discovery process. With the new unified software, the process is the same for IAP and CAP. Actually, with the new unified software, there is no IAP or CAP anymore. The Aruba discovery process is a simple process. The AP uses this process to find a controller or a way to connect to AirWave or Central. Once, the AP found a controller, AirWave or Central it never uses the process again. Except, you do a factory reset on the AP. <pre> Value: 001700180034 Requested Option code: DNS recursive name server (23) Requested Option code: Domain Search List (24) Requested Option code: CAPWAP Access Controllers (52) » Elapsed time » Identity Association for Non-temporary Address </pre> Source: https://www.flomain.de/2018/02/unified-aruba-controller-discovery/

CONFIDENTIAL

Claim 4	ACCUSED PRODUCTS
selecting a 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;	The Accused Products select a control node of said one or more control nodes based on the discovery response messages sent by the control nodes in response to said discovery request message. The discovery response messages include information of the functions offered by the associated control node. Enable Controller Discovery An AP can discover the IP address of the controller from a DNS server, from a DHCP server, or using the Aruba Discovery Protocol (ADP). <u>At boot time, the AP builds a list of controller IP addresses and then tries these addresses in order until it successfully reaches a controller.</u> This list of IP addresses provides an enhanced redundancy scheme for controllers that are located in multiple data centers separated across Layer-3 networks. The AP constructs its list of controller addresses as follows: • If the master provisioning parameter is set to a DNS name, that name is resolved and all resulting addresses are put on the list. If master is set to an IP address, that address is put on the list. • If the master provisioning parameter is not set and a controller address was received in DHCP Option 43, that address is put on the list. • If the master provisioning parameter is not set and no address was received via DHCP option 43, ADP is used to discover a controller address and that address is put on the list. • Controller addresses derived from the server-name and server-ip provisioning parameters and the default controller name aruba-master are added to the list. Note that if a DNS name resolves to multiple addresses, all addresses are added to the list. Controller Discovery using DNS When using DNS, AP learns multiple IP addresses to associate with a controller. If the primary controller is unavailable or does not respond, the AP continues through the list of learned IP addresses until it establishes a connection with an available controller. This takes approximately 3.5 minutes per controller.  NOTE It is recommended you use a DNS server to provide APs with the IP address of the master controller 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 master controller. For the DNS server to resolve this host name to the IP address of the master controller, you must configure an entry on the DNS server for the name aruba-master. Controller Discovery using ADP <u>ADP is enabled by default on all Aruba APs and controllers.</u> With ADP, APs send out periodic multicast and broadcast queries to locate the master controller. ADP requires that all APs and controllers 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. Issue the command show adp config to verify that ADP and IGMP join options are enabled on the controller. If ADP is not enabled, you can reenable 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 master controller, you enable multicast on the network (ADP multicast queries are sent to the IP multicast group address 239.0.82.11) <u>for the controller to respond to the APs' queries. You also must make sure that all routers are configured to listen for Internet Group Management Protocol (IGMP) join requests from the controller and can route these multicast packets.</u> C Controller discovery using a DHCP Server You can configure a DHCP server to provide the master controller's IP address. You must configure the DHCP server to send the controller'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 controller'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 controller 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 <u>"DHCP with Vendor-Specific Options" on page 1</u> or refer to the documentation included with your server. Source: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/AP_Config/AP_discovery_ADp.htm

CONFIDENTIAL

20

U.S. Patent No. 8,270,384

Claim 4	ACCUSED PRODUCTS
selecting a 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;	The Accused Products select a control node of said one or more control nodes based on the discovery response messages sent by the control nodes in response to said discovery request message. The discovery response messages include information of the functions offered by the associated control node. Controller-based AP in a Test Network Users can provision controller-based APs in a test network before deploying the APs in a working network.  NOTE Controllers in a test network can only be discovered using the Aruba Discovery Protocol (ADP). APs are upgraded to the ArubaOS image via ADP through the following steps: 1. The AP boots up with the manufacturing image in unprovisioned mode. 2. The AP enters the controller discovery process using ADP. 3. When a controller is discovered, <u>the AP connects to the controller and downloads the ArubaOS image.</u> ▪ If the AP cannot locate a controller, it enters the Instant discovery process. To prevent the AP from upgrading to controller-less mode, you must make sure Instant VCs, Activate, AirWave, and Central are not available to the AP. If the AP is not upgraded and there are no configuration changes with 15 minutes, the AP reboots and restarts the discovery process (step 1). 4. After the image is downloaded, the AP reboots. 5. The configuration syncs, and the AP runs in controller-based mode. Source: https://www.arubanetworks.com/techdocs/ArubaOS_6_5_4_X_Web_Help/Content/ArubaFrameStyles/AP_Config/AP_Discovery_Logic.htm#controller_manual

CONFIDENTIAL

21

Claim 4	ACCUSED PRODUCTS
selecting a 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;	The Accused Products select a control node of said one or more control nodes based on the discovery response messages sent by the control nodes in response to said discovery request message. The discovery response messages include information of the functions offered by the associated control node. 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) <u>for the Mobility Master to respond to the APs' queries</u>. 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. Source: https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/access-points/enab-ctrl-disc.htm

CONFIDENTIAL

22

U.S. Patent No. 8,270,384

Claim 4	ACCUSED PRODUCTS
establishing a secure session with said selected one control node; and	The Accused Products establish a secure session with said selected one control node. TRUSTED TRAFFIC With the foundation of device assurance delivered by the extensive use of hardware-enforced and monitored protection, <u>Aruba Secure Infrastructure then adds Trusted Traffic functionality to further secure the network.</u> 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. <u>Centralized encryption</u> 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 <u>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.</u> 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.

Source: https://www.arubanetworks.com/assets/so/SO_SecureInfrastructure.pdf

CONFIDENTIAL

Claim 4	ACCUSED PRODUCTS
exchanging information about the functions to be separated between said selected one control node and said wireless point.	The Accused Products exchange information about the functions to be separated between one control node and said wireless point. 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) <u>for the Mobility Master to respond to the APs' queries</u>. 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. Source: https://www.arubanetworks.com/techdocs/ArubaOS_87_Web_Help/Content/arubaos-solutions/access-points/enab-ctrl-disc.htm

CONFIDENTIAL

24

U.S. Patent No. 8,270,384

Claim 4	ACCUSED PRODUCTS
exchanging information about the functions to be separated between said selected one control node and said wireless point.	The Accused Products exchange information about the functions to be separated between one control node and said wireless point. Controller-based AP in a Test Network Users can provision controller-based APs in a test network before deploying the APs in a working network.  NOTE Controllers in a test network can only be discovered using the Aruba Discovery Protocol (ADP). APs are upgraded to the ArubaOS image via ADP through the following steps: 1. The AP boots up with the manufacturing image in unprovisioned mode. 2. The AP enters the controller discovery process using ADP. 3. When a controller is discovered, <u>the AP connects to the controller and downloads the ArubaOS image.</u> ▪ If the AP cannot locate a controller, it enters the Instant discovery process. To prevent the AP from upgrading to controller-less mode, you must make sure Instant VCs, Activate, AirWave, and Central are not available to the AP. If the AP is not upgraded and there are no configuration changes with 15 minutes, the AP reboots and restarts the discovery process (step 1). 4. After the image is downloaded, the AP reboots. 5. The configuration syncs, and the AP runs in controller-based mode. Source: https://www.arubanetworks.com/techdocs/ArubaOS_6_5_4_X_Web_Help/Content/ArubaFrameStyles/AP_Config/AP_Discovery_Logic.htm#controller_manual

CONFIDENTIAL

25

U.S. Patent No. 8,270,384

Claim 4	ACCUSED PRODUCTS
exchanging information about the functions to be separated between said selected one control node and said wireless point.	The Accused Products exchange information about the functions, such as policy configuration information, to be separated between one control node and said wireless point. 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. Source: https://www.arubanetworks.com/vrd/ControllerVRD/wwhelp/wwhimpl/common/html/wwhelp.htm#context=ControllerVRD&file=Chap2.html

CONFIDENTIAL

26

U.S. Patent No. 8,270,384

Claim 6	ACCUSED PRODUCTS
The method according to claim 4, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.	The functions of claim 4 comprise at least Authentication. TRUSTED TRAFFIC With the foundation of device assurance delivered by the extensive use of hardware-enforced and monitored protection, <u>Aruba Secure Infrastructure then adds Trusted Traffic functionality to further secure the network.</u> 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. <u>Centralized encryption</u> 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 <u>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.</u> 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.

Source: https://www.arubanetworks.com/assets/so/SO_SecureInfrastructure.pdf

CONFIDENTIAL

27

U.S. Patent No. 8,270,384

Claim 6	ACCUSED PRODUCTS
The method according to claim 4, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.	The functions of claim 4 comprise at least Authentication. Internet Engineering Task Force (IETF) Request for Comments: 6125 Category: Standards Track ISSN: 2070-1721 P. Saint-Andre Cisco J. Hodges 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 <u>MUST include one or more XMPP addresses (i.e., domainparts) associated with XMPP services hosted at the server.</u> The rules and guidelines defined in [this specification] apply to XMPP server certificates, with the following XMPP-specific considerations: Source: https://www.rfc-editor.org/rfc/rfc6125.txt

CONFIDENTIAL

28

Claim 6	ACCUSED PRODUCTS
The method according to claim 4, wherein said functions for the wireless local area network comprise at least one of Beacon Signal Control, Power Management, Quality of Service (QoS), Scheduling, Authentication, and Encryption/Decryption.	The functions of claim 4 comprise at least Authentication. 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. <u>Aruba Central supports the following external authentication servers:</u> ▪ RADIUS ▪ LDAP Source: https://help.central.arubanetworks.com/2.5.3/documentation/online_help/content/access-points/cfg/security/auth_servers.htm 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. <u>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).</u>  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. Source: https://www.arubanetworks.com/techdocs/ArubaOS_64_Web_Help/Content/ArubaFrameStyles/Management_Uilities/Managing_Certificates.htm

CONFIDENTIAL

29

APPENDIX A TO EXS. B & C

Model No.	Part No.
AP-503H	R3V38A
AP-503H	R7G97A
AP-505H	R3V48A
AP-505H	R3V57A
AP-503H	R3V39A
AP-505H	R3V49A
AP-303H	JZ088A
AP-303H	JY680A
AP-303H	JY681A
AP-203R	JY714A
AP-203R	JY715A
AP-203RP	JY722A
AP-203RP	JY723A
AP-655	R7J39A
AP-655	R7J44A
AP-635	R7J28A
AP-635	R7J33A
AP-615	R7J50A
AP-615	R7J55A
AP-555	JZ357A
AP-555	JZ367A
AP-535	JZ337A
AP-534	JZ332A
AP-535	JZ347A
AP-534	JZ342A
AP-515	Q9H63A
AP-514	Q9H58A
AP-515	Q9H73A

APPENDIX A TO EXS. B & C

AP-514	Q9H68A
AP-505	R2H29A
AP-504	R2H23A
AP-505	R2H39A
AP-504	R2H34A
AP-344	JZ023A
AP-344	JZ024A
AP-345	JZ033A
AP-345	JZ034A
AP-303	JZ321A
AP-303P	R0G69A
AP-303P	R2H45A
AP-584	R7S99A
AP-585	R7T04A
AP-587	R7T09A
AP-584	R7T14A
AP-585	R7T19A
AP-587	R7T24A
AP-585EX	R7T29A
AP-587EX	R7T34A
AP-574	R4H13A
AP-575	R4H18A
AP-577	R4H23A
AP-574	R4H28A
AP-575	R4H33A
AP-577	R4H38A
AP-575EX	R4W34A
AP-577EX	R4W39A
AP-565	R4W44A

APPENDIX A TO EXS. B & C

AP-567	R4W49A
AP-565	R4W54A
AP-567	R4W59A
AP-565EX	R4W63A
AP-567EX	R4W67A
AP-518	R4H03A
AP-518	R4H08A
AP-387	R0K14A
AP-387	R4E11A
AP-374	JZ163A
AP-375	JZ173A
AP-377	JZ183A
AP-374	JZ168A
AP-375	JZ178A
AP-377	JZ188A
AP-375EX	R3P69A
AP-377EX	R3P90A
AP-375ATEX	R7J11A
AP-365	JX967A
AP-365	JZ969A
AP-367	JX974A
AP-367	JX976A
AP-318	JZ153A
AP-318	JZ158A
9240	R7H95A
9240	R7J02
9004	R1B20A
9004	R1B25A
9012	R1B31A

APPENDIX A TO EXS. B & C

9012	R1B36A
7205	JW736A
7205	JW740A
7210	JW744A
7210DC	JW646A
7210	JW746A
7220	JW752A
7220DC	JW650A
7220	JW754A
7240XM	JW784A
7240XM	JW830A
7240XMDC	JW675A
7280	JX910A
7280	JX914A
7010	JW679A
7010	JW703A
7030	JW687A
7030	JW711A
7005	JW634A
7005	JW636A
7008	JX928A
7008	JX932A
Aruba MCR-HW-1K Mobility Conductor Hardware Appliance	JY791A
Aruba MCR-HW-5K Mobility Conductor Hardware Appliance	JY792A
Aruba MCR-HW-10K Mobility Conductor Hardware Appliance	JY793A
Aruba MCR-HW-1K-F1 Mobility Conductor Hardware Appliance FIPS/TAA	JZ396A
Aruba MCR-HW-5K-F1 Mobility Conductor Hardware Appliance FIPS/TAA	JZ397A
Aruba MCR-HW-10K-F1 Mobility Conductor Hardware Appliance FIPS/TAA	JZ398A
Aruba LIC-AP Controller per AP Capacity License E-LTU	JW472AAE

APPENDIX A TO EXS. B & C

Aruba LIC-PEF Controller Policy Enforcement Firewall per AP License E-LTU	JW473AAE
Aruba LIC-RFP Controller RFProtect per AP License E-LTU	JW474AAE
Aruba LIC-ENT Enterprise (LIC-AP LIC-PEF LIC-RFP and LIC-AW) License Bundle E-LTU	JW471AAE
Aruba LIC-ACR Controller Advanced Cryptography 1 Session License E-LTU	Q9B90AAE
Aruba Controller Web Content Classification 1 Year Subscription E-STU	JY028AAE
Aruba Controller Web Content Classification 3 Year Subscription E-STU	JY029AAE
Aruba Controller Web Content Classification 5 Year Subscription E-STU	JY030AAE
Aruba Controller Web Content Classification 7 Year Subscription E-STU	JY031AAE
Aruba Controller Web Content Classification 10 Year Subscription E-STU	JY032AAE
Aruba LIC-VIA per VIA Client License E-LTU	JZ148AAE
Aruba MC-VA-10 Virtual Mobility Controller License (US)	Q9B95AAE
Aruba MC-VA-10 Virtual Mobility Controller License (USF1)	Q9B59AAE
Aruba MC-VA-50 Virtual Mobility Controller License (US)	JY902AAE
Aruba MC-VA-50 Virtual Mobility Controller License (USF1)	JZ392AAE
Aruba MC-VA-250 Virtual Mobility Controller License (US)	JY903AAE
Aruba MC-VA-250 Virtual Mobility Controller License (USF1)	JZ393AAE
Aruba MC-VA-1K Virtual Mobility Controller License (US)	JY904AAE
Aruba MC-VA-1K Virtual Mobility Controller License (USF1)	JZ394AAE

Ex. D - U.S. Patent No. 8,467,723

HPE makes, uses, tests, offers for sale, sells, and/or imports devices that support inter-RAT handovers (the “Accused Products”). Each of the Accused Products include the features identified in this chart. The features and functionality identified in this chart cause the Accused Products to practice the asserted claims of U.S. Patent No. 8,467,723 (the “’723 patent”). The Accused Products include any LTE device that HPE makes, uses, tests, offers for sale, sells, and/or imports that supports inter-RAT handovers. The Accused Products include, but are not limited to, HPE’s LTE gateways, including, but not limited to, the following devices:

- Aruba 9004-LTE Devices
- Aruba USB LTE Modem
- Aruba SD-WAN Backpack LTE Solution

The specific ways in which the Accused Products support inter-RAT handovers will be detailed in documents and/or source code that is produced in discovery. SPV reserves the right to supplement this contention upon receipt of such discovery.

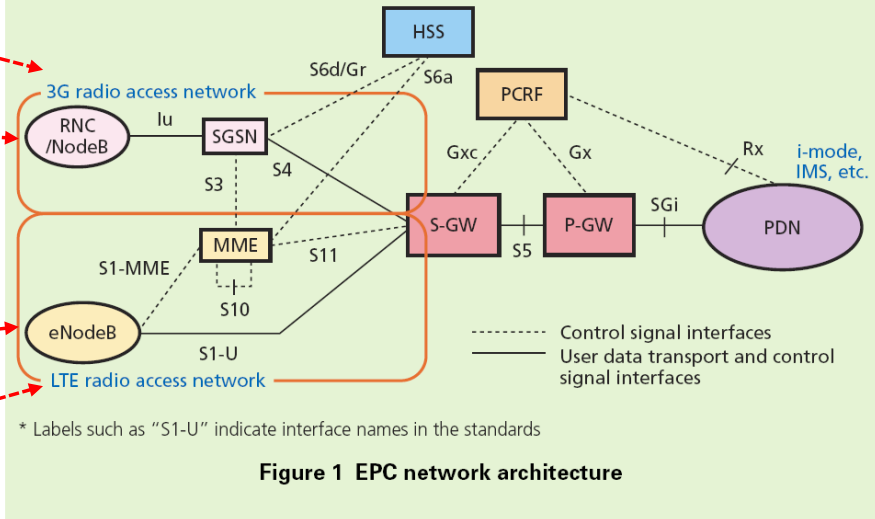
The above list is not intended to be exhaustive. HPE directly infringes the asserted claims of the ’723 patent because the Accused Products comprise or perform all elements of the asserted claims. Among other things, HPE practices the asserted method claims by testing the Accused Products. Further, the operation of the Accused Products on a cellular network is done under the direction or control of HPE. For example, HPE deploys the Accused Products with built-in firmware to perform inter-RAT handover. This firmware controls the operation of the Accused Products and cannot be altered by end users. HPE also indirectly infringes the asserted claims of the ’723 patent by encouraging its customers and end-users to deploy the Accused Products in an LTE network that supports inter-RAT handovers, creating advertisements that promote infringing use, maintaining distribution channels for the Accused Products, distributing or making available instructions or manuals for the Accused Products, and providing technical support, replacement parts, or services for the Accused Products. Moreover, the Accused Products contain instructions, such as executable firmware, that cause the device to infringe the asserted claims.

CONFIDENTIAL

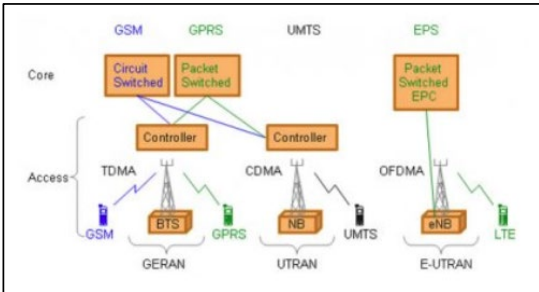
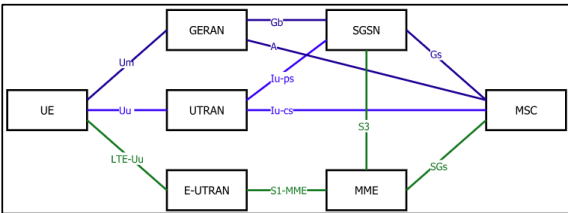
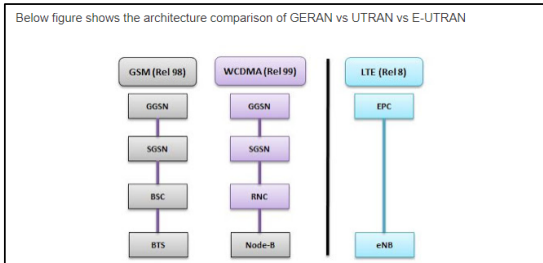
Claim 5	ACCUSED PRODUCTS																		
A mobile station apparatus that belongs to a first area which is covered by a base station apparatus employing a first Radio Access Technology (RAT), the first area including part or entirety of a second area which is covered by a host station employing a second RAT different from the first RAT, the mobile station apparatus comprising:	Each Accused Product is a mobile station apparatus. For example, the Accused Products include, but are not limited to the Aruba 9004-LTE Gateway. The Accused Products operate in accordance with 3GPP standards, including all versions of each standard referenced herein. Each Accused Product is User Equipment ("UE") as defined by 3GPP.  Integrated LTE ^ AVAILABLE ON THE 9004-LTE ONLY <table> <tr> <td>Downlink/Uplink Speed</td><td>600/150 Mbps</td></tr> <tr> <td>LTE Category</td><td>12</td></tr> <tr> <td>Connectors</td><td>2xSMA connectors for Main and Diversity Antenna 1xSMA connector for GPS Antenna</td></tr> </table> BANDS SUPPORTED <table> <tr> <td>Regions Supported</td><td>Global</td></tr> <tr> <td>LTE-FDD</td><td>B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20/B21/B25/B26/B28/B29/B30/B32/B66</td></tr> <tr> <td>LTE-TDD</td><td>B38/B39/B40/B41</td></tr> <tr> <td>2 x CA</td><td>B1+B3/B5/B18/B19/B20/B21/B26; B2+B2/B4/B5/B12/B13/B17/B29/B30/B66; B3+B3/B5/B7/B8/B9/B20/B28; B4+B4/B5/B12/B13/B17/B25/B30; B5+B7/B25/B30/B66; B7+B7/B20/B28; B12+B25/B30; B13+B66; B20+B32; B25+B25/B26/B41; B29+B30; B38+B38; B40+B40; B41+B41; B66+B66</td></tr> <tr> <td>3 x CA</td><td>DL inter-band 3CA: B1+B3+B7; B1+B3+B19; B1+B3+B20; B1+B19+B21; B2+B4+B5; B2+B4+B13; B2+B5+B30; B2+B12+B30; B2+B29+B30; B3+B7+B20; B3+B7+B28; B4+B5+B30; B4+B12+B30; B4+B29+B30; B5+B66+B2; B13+B66+B2 DL 2 contiguous plus inter-band 3CA: B2+B2+B5; B2+B2+B13; B3+B3+B7; B3+B7+B7; B3+B3+B20; B4+B4+B5; B4+B4+B13; B5+B66+B66; B13+B66+B66; B66+B66+B2; B66+B66+B66</td></tr> <tr> <td>UMTS</td><td>B1/B2/B3/B4/B5/B8/B19</td></tr> </table> https://www.arubanetworks.com/products/wireless/gateways-and-controllers/9000-series/	Downlink/Uplink Speed	600/150 Mbps	LTE Category	12	Connectors	2xSMA connectors for Main and Diversity Antenna 1xSMA connector for GPS Antenna	Regions Supported	Global	LTE-FDD	B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20/B21/B25/B26/B28/B29/B30/B32/B66	LTE-TDD	B38/B39/B40/B41	2 x CA	B1+B3/B5/B18/B19/B20/B21/B26; B2+B2/B4/B5/B12/B13/B17/B29/B30/B66; B3+B3/B5/B7/B8/B9/B20/B28; B4+B4/B5/B12/B13/B17/B25/B30; B5+B7/B25/B30/B66; B7+B7/B20/B28; B12+B25/B30; B13+B66; B20+B32; B25+B25/B26/B41; B29+B30; B38+B38; B40+B40; B41+B41; B66+B66	3 x CA	DL inter-band 3CA: B1+B3+B7; B1+B3+B19; B1+B3+B20; B1+B19+B21; B2+B4+B5; B2+B4+B13; B2+B5+B30; B2+B12+B30; B2+B29+B30; B3+B7+B20; B3+B7+B28; B4+B5+B30; B4+B12+B30; B4+B29+B30; B5+B66+B2; B13+B66+B2 DL 2 contiguous plus inter-band 3CA: B2+B2+B5; B2+B2+B13; B3+B3+B7; B3+B7+B7; B3+B3+B20; B4+B4+B5; B4+B4+B13; B5+B66+B66; B13+B66+B66; B66+B66+B2; B66+B66+B66	UMTS	B1/B2/B3/B4/B5/B8/B19
Downlink/Uplink Speed	600/150 Mbps																		
LTE Category	12																		
Connectors	2xSMA connectors for Main and Diversity Antenna 1xSMA connector for GPS Antenna																		
Regions Supported	Global																		
LTE-FDD	B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20/B21/B25/B26/B28/B29/B30/B32/B66																		
LTE-TDD	B38/B39/B40/B41																		
2 x CA	B1+B3/B5/B18/B19/B20/B21/B26; B2+B2/B4/B5/B12/B13/B17/B29/B30/B66; B3+B3/B5/B7/B8/B9/B20/B28; B4+B4/B5/B12/B13/B17/B25/B30; B5+B7/B25/B30/B66; B7+B7/B20/B28; B12+B25/B30; B13+B66; B20+B32; B25+B25/B26/B41; B29+B30; B38+B38; B40+B40; B41+B41; B66+B66																		
3 x CA	DL inter-band 3CA: B1+B3+B7; B1+B3+B19; B1+B3+B20; B1+B19+B21; B2+B4+B5; B2+B4+B13; B2+B5+B30; B2+B12+B30; B2+B29+B30; B3+B7+B20; B3+B7+B28; B4+B5+B30; B4+B12+B30; B4+B29+B30; B5+B66+B2; B13+B66+B2 DL 2 contiguous plus inter-band 3CA: B2+B2+B5; B2+B2+B13; B3+B3+B7; B3+B7+B7; B3+B3+B20; B4+B4+B5; B4+B4+B13; B5+B66+B66; B13+B66+B66; B66+B66+B2; B66+B66+B66																		
UMTS	B1/B2/B3/B4/B5/B8/B19																		

CONFIDENTIAL

2

Claim 5	ACCUSED PRODUCTS
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, the mobile station apparatus comprising:	Each Accused Product 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. For example, the Accused Products operate on LTE and other RAT systems. The Evolved Packet Core ("EPC"), the core network of the LTE system, supports multiple access technologies and allows for handover between these accesses, including accommodation of LTE and 3G as shown in the figure below. In EPC, the Serving Gateway ("S-GW") transports IP data traffic between the User Equipment ("UE") (such as the Accused Products) and the external networks and is the point of interconnect between the radio-side and the EPC. The S-GW is the anchor point for the inter-RAT mobility (such as in case of handover between LTE and other 3GPP accesses).  Figure 1 EPC network architecture Source: https://www.cultofmac.com/421369/; https://www.docomo.ne.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol11_3/vol11_3_004en.pdf

CONFIDENTIAL

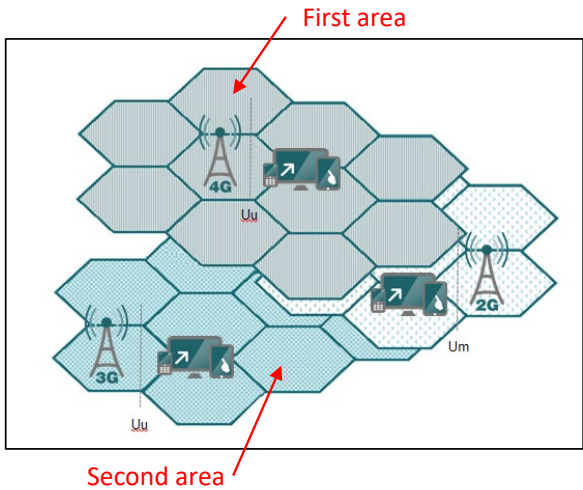
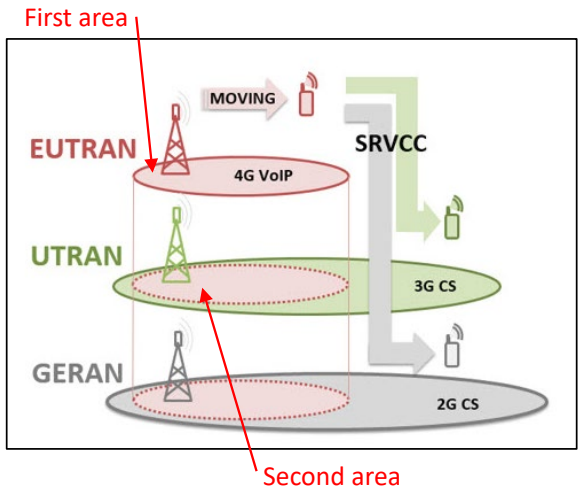
Claim 5	ACCUSED PRODUCTS																																
A mobile station apparatus that belongs to a first area which is covered by a base station apparatus employing a first Radio Access Technology (RAT), the first area including part or entirety of a second area which is covered by a host station employing a second RAT different from the first RAT, the mobile station apparatus comprising:	In accordance with 3GPP specifications, the Accused Products support inter-RAT handover of a UE between LTE radio access networks (E-UTRAN) and radio access networks using older generation radio access technologies such as UTRAN (3G), UMTS (3G GSM), GPRS (GSM 2G, 3G packet mobile data), and GERAN (3G GSM EDGE RAN). For example, the figures below depict features of the different RAN, how they coexist, and how they are arranged.  Source: https://www.techplayon.com/lte-overview/  Source: https://upload.wikimedia.org/wikipedia/en/a/af/LTE-CSFB-E-UTRAN-UTRAN-GERAN-Interfaces.svg																																
	Below figure shows the architecture comparison of GERAN vs UTRAN vs E-UTRAN  GERAN vs UTRAN vs E-UTRAN Design Comparison Refer the below mentioned table for design comparison GERAN vs UTRAN vs E-UTRAN <table><tr><th>Comparison</th><th>GERAN</th><th>UTRAN</th><th>LTE</th></tr><tr><td>Radio Access</td><td>FDMA/TDMA</td><td>WCDMA</td><td>OFDMA/SC-FDMA</td></tr><tr><td>Bandwidth</td><td>200KHz</td><td>5MHz</td><td>1.4,3,5,10,15,20 MHz</td></tr><tr><td>Data Rate</td><td>14.4Kbps ~ 1.89Mbps</td><td>384Kbps~42Mbps</td><td>300Mbps</td></tr><tr><td>Mobility (KM/Hr)</td><td>100</td><td>120</td><td>350</td></tr><tr><td>Latency</td><td>700 ~ 180ms</td><td>220~110ms</td><td>< 100ms for Control Plane < 5ms for Data Plane</td></tr><tr><td>Services</td><td>Both circuit & packet switched</td><td>Both circuit & packet switched</td><td>Packet Switched only</td></tr><tr><td>Architecture</td><td>4 NW nodes (not flat)</td><td>4 NW nodes (not flat)</td><td>2 NW nodes (flat)</td></tr></table> Design Comparison Source: https://wirelessworld5g.com/geran-utran-comparison-with-lte/	Comparison	GERAN	UTRAN	LTE	Radio Access	FDMA/TDMA	WCDMA	OFDMA/SC-FDMA	Bandwidth	200KHz	5MHz	1.4,3,5,10,15,20 MHz	Data Rate	14.4Kbps ~ 1.89Mbps	384Kbps~42Mbps	300Mbps	Mobility (KM/Hr)	100	120	350	Latency	700 ~ 180ms	220~110ms	< 100ms for Control Plane < 5ms for Data Plane	Services	Both circuit & packet switched	Both circuit & packet switched	Packet Switched only	Architecture	4 NW nodes (not flat)	4 NW nodes (not flat)	2 NW nodes (flat)
Comparison	GERAN	UTRAN	LTE																														
Radio Access	FDMA/TDMA	WCDMA	OFDMA/SC-FDMA																														
Bandwidth	200KHz	5MHz	1.4,3,5,10,15,20 MHz																														
Data Rate	14.4Kbps ~ 1.89Mbps	384Kbps~42Mbps	300Mbps																														
Mobility (KM/Hr)	100	120	350																														
Latency	700 ~ 180ms	220~110ms	< 100ms for Control Plane < 5ms for Data Plane																														
Services	Both circuit & packet switched	Both circuit & packet switched	Packet Switched only																														
Architecture	4 NW nodes (not flat)	4 NW nodes (not flat)	2 NW nodes (flat)																														

CONFIDENTIAL

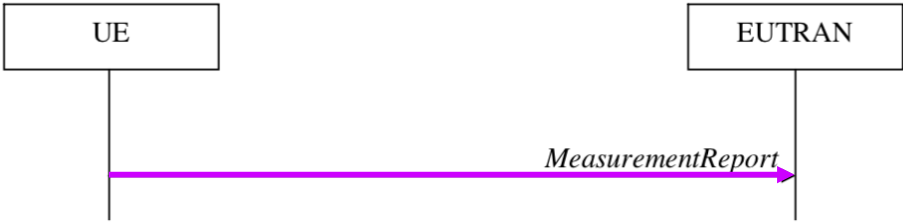
Claim 5	ACCUSED PRODUCTS
A mobile station apparatus that belongs to a first area which is covered by a base station apparatus employing a first Radio Access Technology (RAT), the first area including part or entirety of a second area which is covered by a host station employing a second RAT different from the first RAT, the mobile station apparatus comprising:	An inter-RAT handover occurs when the mobile station's radio connection is switched from the base station (e.g., LTE eNB) employing a first RAT (e.g., LTE) to a host station (e.g., RNC/NodeB) employing a second RAT (e.g., 3G). RAT handover scenarios include: (i) between E-UTRAN (LTE) and UTRAN or GERAN (both 3G) and (ii) between MTS (3G UTRAN) and GERAN (3G). <u>Inter-RAT handover</u>: indicates the transfer of the connection, under the control of the network, between the MS and two different radio access technologies (e.g. UMTS to GERAN Iu mode). Source: 3GPP TS 44.118 version 15.0.0 Release 15 5.5.2.1 <u>E-UTRAN to UTRAN Iu mode Inter RAT handover</u> 5.5.2.1.1 General 1. <u>The source eNodeB decides to initiate an Inter-RAT handover to the target access network, UTRAN Iu mode.</u> At this point both uplink and downlink user data is transmitted via the following: Bearer(s) between UE and source eNodeB, GTP tunnel(s) between source eNodeB, Serving GW and PDN GW. If the UE has an ongoing emergency bearer service the source eNodeB shall not initiate PS handover to a UTRAN cell that is not IMS voice capable. Source: 3GPP TS 23.401 version 15.6.0 Release 15 "MS" =  "mobile station"

CONFIDENTIAL

5

Claim 5	ACCUSED PRODUCTS
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, the mobile station apparatus comprising:	The first area includes part or entirety of a second area which is covered by a host station employing a second RAT different from the first RAT. For example, for each carrier operating in an area, the areas covered by different RAT overlap with one another according to where the carriers' eNB/NodeB/RNC are located (see below, left). For economies of scale and cost savings, many carriers deploy their eNB/NodeB/RNC from the same physical location (for example, a cell tower), thus resulting in a direct overlapping RAT area in the vicinity of the deployment (see below, right). The Accused Products are configured to operate pursuant to both of these examples. For example, cellular providers utilizes tower that employ multiple RAT, thus providing an overlapping first area for a first RAT (e.g. LTE) and second area for a second RAT (e.g. 3G).  First area Second area Source: https://www.primatelecomtesting.com/solutions/network-equipment-manufacturers/ran-testing/inter-rat-ho-testing/  First area Second area Source: https://www.netmanias.com/en/?m=view&id=blog&no=10908

CONFIDENTIAL

Claim 5	ACCUSED PRODUCTS
a transmitter configured to 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, and	Each Accused Product includes a transmitter configured to transmit, to the base station apparatus, notification information while the mobile station apparatus is using the first RAT. For example, E-UTRAN UEs (such as the Accused Products) include a transmitter to transmit notification information (e.g., measurement information) to the base station apparatus (e.g., the E-UTRAN eNB) while using the first RAT (e.g., LTE). 5.5 Measurements 5.5.1 Introduction <u>The UE reports measurement information in accordance with the measurement configuration as provided by E-UTRAN.</u> E-UTRAN provides the measurement configuration applicable for a UE in RRC_CONNECTED by means of dedicated signalling, i.e. using the <i>RRCConnectionReconfiguration</i> message. Source: 3GPP TS 36.331 version 11.19.0 Release 11 5.5.5 Measurement reporting  <pre> sequenceDiagram participant UE participant EUTRAN UE->>EUTRAN: MeasurementReport </pre> Figure 5.5.5-1: Measurement reporting Source: 3GPP TS 36.331 version 11.19.0 Release 11

CONFIDENTIAL

7

Claim 5	ACCUSED PRODUCTS
a transmitter configured to 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, and	Each Accused Products' transmitter is configured to transmit notification information when the mobile station apparatus detects that the mobile station apparatus is located in the second area while using the first RAT. For example, in the 4G-to-3G use case, the E-UTRAN UEs report measurement information for multiple types of RAT cells according to the UE's measurement configuration. Further, when a E-UTRAN UE detects that it is located in the second area while using the first RAT (e.g., the UE is within a 3G radio cell while still connected to its LTE eNB) the UE will procure measurement data for the cells of the second area. 5.5 Measurements 5.5.1 Introduction <u>The UE reports measurement information in accordance with the measurement configuration as provided by E-UTRAN.</u> E-UTRAN provides the measurement configuration applicable for a UE in RRC_CONNECTED by means of dedicated signalling, i.e. using the <i>RRCConnectionReconfiguration</i> message. The measurement procedures <u>distinguish the following types of cells:</u> 1. <u>The serving cell(s)</u>– these are the PCell and one or more SCells, if configured for a UE supporting CA. 2. <u>Listed cells</u> - these are cells listed within the measurement object(s). 3. <u>Detected cells</u> - these are cells that are not listed within the measurement object(s) but are detected by the UE on the carrier frequency(ies) indicated by the measurement object(s). Source: 3GPP TS 36.331 version 11.19.0 Release 11

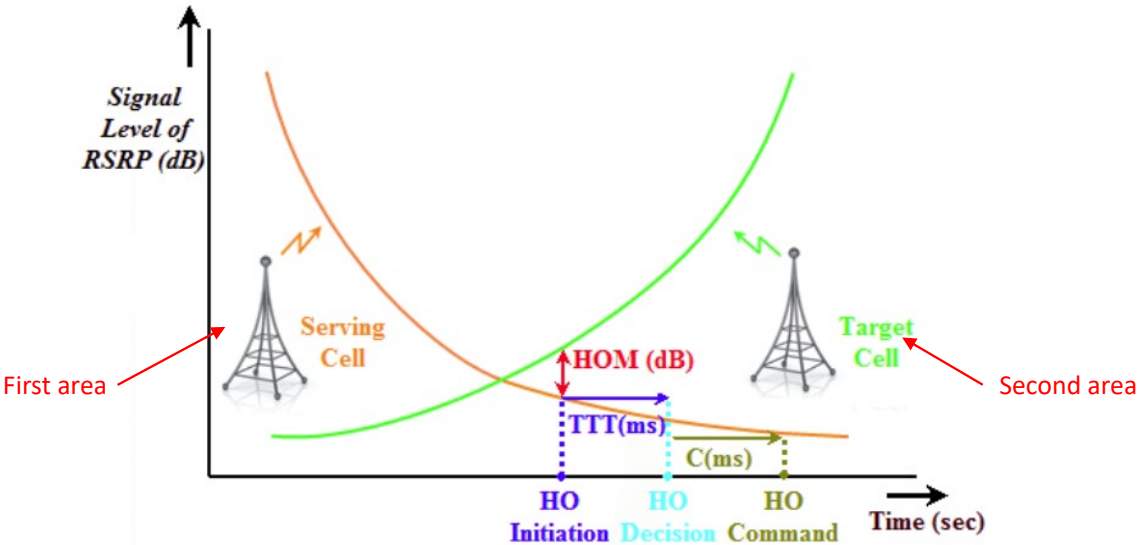
CONFIDENTIAL

8

U.S. Patent No. 8,467,723

Claim 5	ACCUSED PRODUCTS
a transmitter configured to 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, and	In the 4G-to-3G use case, the UE belongs to an LTE macro cell (a “first area”) covered by an LTE eNB (“a base station apparatus employing a first RAT”). As E-UTRAN UEs measure and report on multiple cells of base/host stations employing various RATs, overlap exists in base/host station cell coverage, and the first area that the E-UTRAN UE belongs to (e.g., covered by 4G LTE eNB, the “base station”) includes part or the entirety of a second area covered by a host station (e.g., a 3G NodeB or RNC). This cell coverage overlap is present during a UE inter-RAT handover. Different types of cells (e.g., serving, listed, detected, and within range) are measured and reported on under the various inter-RAT scenarios. For E-UTRA, the UE measures and reports on the serving cell(s), listed cells and detected cells. For inter-RAT UTRA, the UE measures and reports on listed cells and optionally on cells that are within a range for which reporting is allowed by E-UTRAN. For inter-RAT GERAN, the UE measures and reports on detected cells. For inter-RAT CDMA2000, the UE measures and reports on listed cells. NOTE 2: For inter-RAT UTRA and CDMA2000, the UE measures and reports also on detected cells for the purpose of SON. Source: 3GPP TS 36.331 version 11.19.0 Release 11

CONFIDENTIAL

Claim 5	ACCUSED PRODUCTS
a transmitter configured to 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, and	The diagram below illustrates how a UE moving from the area of a serving cell ("first area" with eNB "base station apparatus") into a separate area covered by a target cell ("second area" with a NodeB or RNC "host station") will experience changing RF signal conditions from each cell. These changing signal conditions (such as the serving cell's signal becoming weaker as the target cell's signal becomes stronger) will trigger the UE handing over from the serving cell ("first area") to the target cell ("second area"). The UE is aware of the changing RF signal conditions based on its measuring the cells' RF signals.  Principle of the LTE hard handover process. Source: https://www.researchgate.net/figure/Principle-of-the-LTE-hard-handover-process_fig1_311642429

CONFIDENTIAL

10

U.S. Patent No. 8,467,723

Claim 5	ACCUSED PRODUCTS
a transmitter configured to 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, and	The UE is aware of the changing RF signal conditions based on its measuring the cells' RF signals. The notification information is transmitted when a UE (such as an Accused Product) detects that it is located in the second area while using the first RAT. In the 4G-to-3G use case, the trigger for the E-UTRAN UE to send notification information (measurement results) to its connected eNB is based on the UE's measurement configuration, which configures the types of inter-RAT neighbor cells to measure and other variables such as thresholds and timing for measurement events. When a UE is within range (in the second area) of the inter-RAT neighbor cell, the UE will take measurements, the results of which, if meeting a configured measurement process, will trigger a handover to the inter-RAT neighbor cell. 5.5.4 Measurement report triggering 5.5.4.7 <u>Event B1 (Inter RAT neighbour becomes better than threshold)</u> The UE shall: 1> for UTRA and CDMA2000, only trigger the event for cells included in the corresponding measurement object; 1> consider the entering condition for this event to be satisfied when condition B1-1, as specified below, is fulfilled; 1> consider the leaving condition for this event to be satisfied when condition B1-2, as specified below, is fulfilled; <u>Inequality B1-1 (Entering condition)</u> $Mn + Ofn - Hys > Thresh$ Inequality B1-2 (Leaving condition) $Mn + Ofn + Hys < Thresh$ The variables in the formula are defined as follows: <u>Mn</u> is the measurement result of the inter-RAT neighbour cell, not taking into account any offsets. For CDMA 2000 measurement result, <i>pilotStrength</i> is divided by -2. <u>Ofn</u> is the frequency specific offset of the frequency of the inter-RAT neighbour cell (i.e. <i>offsetFreq</i> as defined within the <i>measObject</i> corresponding to the frequency of the neighbour inter-RAT cell). <u>Hys</u> is the hysteresis parameter for this event (i.e. <i>hysteresis</i> as defined within <i>reportConfigInterRAT</i> for this event). <u>Thresh</u> is the threshold parameter for this event (i.e. <i>b1-Threshold</i> as defined within <i>reportConfigInterRAT</i> for this event). For CDMA2000, <i>b1-Threshold</i> is divided by -2. Source: 3GPP TS 36.331 version 11.19.0 Release 11

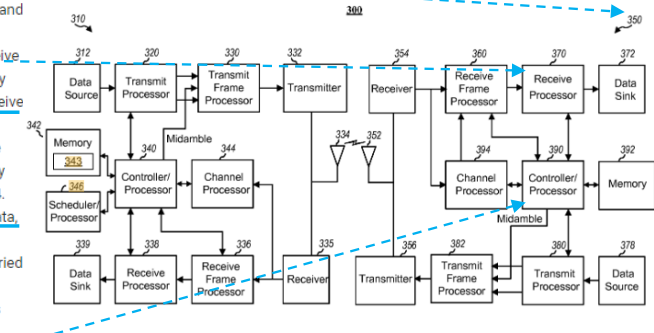
CONFIDENTIAL

11

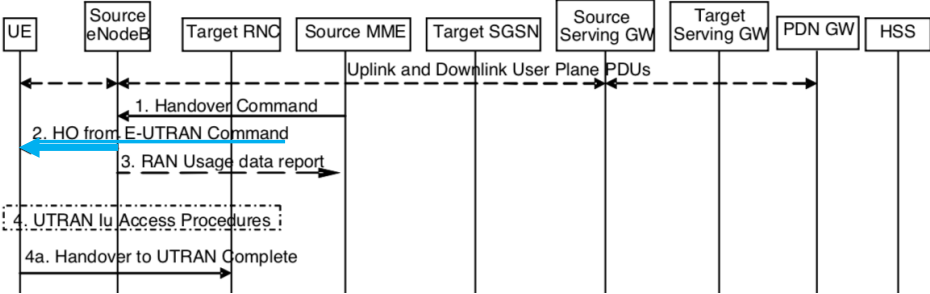
Claim 5	ACCUSED PRODUCTS
a controller configured to perform handover based on traffic control by the base station apparatus using the notification information.	Each Accused Product includes a controller configured to perform the handover based on traffic control by the base station apparatus using the notification information. For example, UEs like the Accused Products have controllers implemented via a hardware and/or software within their mobile platforms. On information and belief, the baseband processor of the Accused Product's cellular modem acts as the claimed controller. High-level, functional information regarding exemplary UE with controllers (as part of mobile platforms, for example, supplied by Qualcomm) is shown below. The diagram illustrates Qualcomm's RF Front End capabilities and architecture. On the left, a table lists 'Capabilities critical for 5G RF success' with a checkmark for each item. The items are: Modem-to-antenna portfolio, Power Amps – MMPA, Power Amps – PAMiDs, LNA/Filter modules, Power tracker, Antenna tuner, Filters – BAW/FBAR, Filters – SAW, Filters – TC-SAW, RF transceiver, Modem, Modem intelligence and SW, and Full system-level solution. On the right, a block diagram shows the 'Qualcomm RF Front End' architecture. It includes a 'Modem' block connected to an 'RF Front End' block. The RF Front End block contains various components: Power Amplifier, Low Noise Amplifier, Filter, Switch, Antenna Tuner, and Antenna. The diagram also shows a '4G' and '5G' section. The 4G section shows a 'Modem' connected to an 'RF Front End' block. The 5G section shows a 'Modem' connected to an 'RF Front End' block, which is further connected to an 'RFFE Controller' and an 'ICVIR' block. The RFFE Controller and ICVIR block are connected to the Modem. The diagram also includes a URL: https://www.qualcomm.com/media/documents/files/making-5g-nr-a-commercial-reality.pdf (slide 31).

CONFIDENTIAL

12

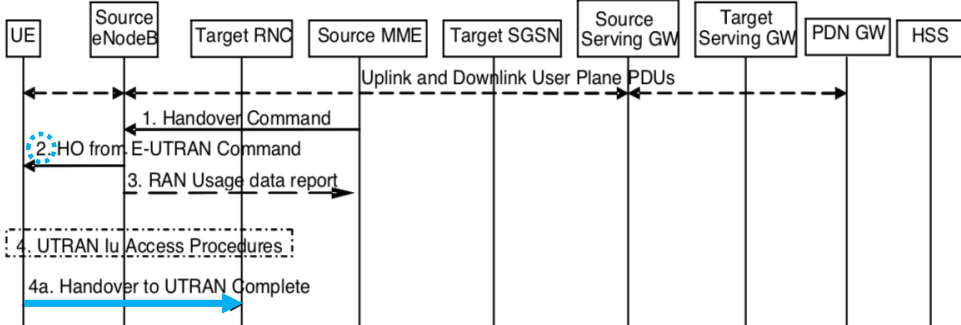
Claim 5	ACCUSED PRODUCTS
a controller configured to perform handover based on traffic control by the base station apparatus using the notification information.	Each Accused Product includes a controller in order to perform the full functionality of the Accused Product, including supporting inter-RAT handovers. The excerpt below is exemplary of a UE having a controller configured to perform handover. As shown, the UE architecture includes a “Receive Processor” and a “Controller/Processor” (370 & 390 in FIG. 3) that enables handover according to a HO command from its serving eNB (see ‘365, FIG. 5). At the UE 350, a receiver 354 receives the downlink transmission through an antenna 352 and processes the transmission to recover the information modulated onto the carrier. The information recovered by the receiver 354 is provided to a receive frame processor 360, which parses each frame, and provides the midamble 214 (FIG. 2) to a channel processor 394 and the data, control, and reference signals to a receive processor 370. The receive processor 370 then performs the inverse of the processing performed by the transmit processor 320 in the Node B 310. More specifically, the receive processor 370 descrambles and despreads the symbols, and then determines the most likely signal constellation points transmitted by the Node B 310 based on the modulation scheme. These soft decisions may be based on channel estimates computed by the channel processor 394. The soft decisions are then decoded and deinterleaved to recover the data, control, and reference signals. The CRC codes are then checked to determine whether the frames were successfully decoded. The data carried by the successfully decoded frames will then be provided to a data sink 372, which represents applications running in the UE 350 and/or various user interfaces (e.g., display). Control signals carried by successfully decoded frames will be provided to a controller/processor 390. When frames are unsuccessfully decoded by the receiver processor 370, the controller/processor 390 may also use an Acknowledgement (ACK) and/or Negative Acknowledgement (NACK) protocol to support retransmission requests for those frames. Source: US Patent 8,792,365  The diagram illustrates the architecture of a User Equipment (UE) 350. It shows two main paths: a transmit path (top) and a receive path (bottom). The transmit path starts with a Data Source (312) connected to a Transmit Processor (320). The Transmit Processor (320) is connected to a Transmit Frame Processor (330), which is connected to a Transmitter (332). The Transmitter (332) is connected to an antenna (352). The receive path starts with an antenna (354) connected to a Receiver (354). The Receiver (354) is connected to a Receive Frame Processor (360), which is connected to a Receive Processor (370). The Receive Processor (370) is connected to a Data Sink (372). A Controller/Processor (390) is connected to the Transmit Processor (320), the Receive Processor (370), and a Memory (342). A Channel Processor (394) is connected to the Transmit Frame Processor (330) and the Receive Frame Processor (360). A Scheduler/Processor (336) is connected to the Transmit Processor (320) and the Receive Processor (370). A Data Sink (338) is connected to the Receive Processor (370). A Data Source (378) is connected to the Transmit Processor (320). A Midamble (344) is connected to the Channel Processor (394). A Receiver (335) is connected to the Transmitter (332). A Transmitter (336) is connected to the Receiver (354). A Transmitter (362) is connected to the Receive Frame Processor (360). A Transmitter (366) is connected to the Receive Processor (370).

CONFIDENTIAL

Claim 5	ACCUSED PRODUCTS
a controller configured to perform handover based on traffic control by the base station apparatus using the notification information.	Each Accused Products' controller is configured to perform handover based on traffic control by the base station apparatus using the notification information. For example, in the 4G-to-3G use case, the UE's controller is responsive to ("configured to") a HO (handover) message received from its LTE eNB ("perform handover based on traffic control by the base station apparatus using the notification information"), based on the UE's measurement configuration and its reported measurement results. 5.5.2.1 <u>E-UTRAN to UTRAN lu mode Inter RAT handover</u> 5.5.2.1.3 <u>Execution phase</u>  2. <u>The source eNodeB will give a command to the UE to handover to the target access network via the message HO from E-UTRAN Command.</u> This message includes a transparent container including radio aspect parameters that the target RNC has set-up in the preparation phase. The details of this E-UTRAN specific signalling are described in TS 36.300 [5]. Source: 3GPP TS 23.401 version 15.6.0 Release 15

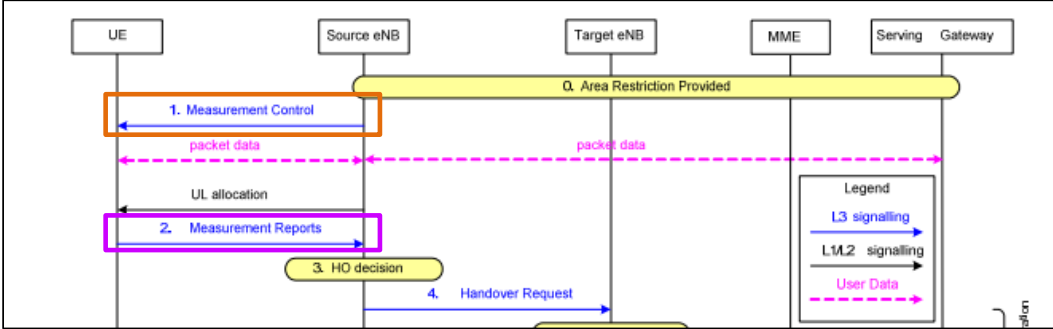
CONFIDENTIAL

14

Claim 5	ACCUSED PRODUCTS
a controller configured to perform handover based on traffic control by the base station apparatus using the notification information.	In the 4G-to-3G use case, the base station performs traffic control for the UE by sending the UE a HO message, which triggers a handover by causing the UE to detach from 4G E-UTRAN and attach to 3G (UTRAN in the diagram below) according to the parameters provided in the HO message. 5.5.2.1 E-UTRAN to UTRAN Iu mode Inter RAT handover 5.5.2.1.3 Execution phase  3GPP TS 23.401 version 15.6.0 Release 15 4. <u>The UE moves to the target UTRAN Iu (3G) system and executes the handover according to the parameters provided in the message delivered in step 2.</u> The procedure is the same as in step 6 and 8 in clause 5.2.2.2 in TS 43.129 [8] with the additional function of association of the received RABs and existing Bearer Id related to the particular NSAPI. Source: 3GPP TS 23.401 version 15.6.0 Release 15

CONFIDENTIAL

15

Claim 6	ACCUSED PRODUCTS
The mobile station apparatus according to claim 5, wherein the mobile station apparatus includes a receiver configured to receive, from the base station apparatus, a request signal for requesting a transmission of the notification information to the base station apparatus, wherein the request signal is received using a broadcast channel from the base station apparatus.	Each Accused Product is a mobile station apparatus that includes a receiver configured to receive, from the base station apparatus, a request signal for requesting a transmission of the notification information to the base station apparatus, wherein the request signal is received using a broadcast channel from the base station apparatus. During the LTE handover process, a UE receives a request signal (e.g., a measurement control signal) from the base station (e.g., the source eNB). When the HO is initiated, the UE sends the notification information (e.g., measurement report) to the source eNB.  Below is a more detailed description of the intra-MME/Serving Gateway HO procedure: 0 The UE context within the source eNB contains information regarding roaming and access restrictions which were provided either at connection establishment or at the last TA update. 1 The source eNB configures the UE measurement procedures according to the roaming and access restriction information and e.g. the available multiple frequency band information. <u>Measurements provided by the source eNB may assist the function controlling the UE's connection mobility.</u> 2 <u>A MEASUREMENT REPORT is triggered and sent to the eNB.</u> 3 <u>The source eNB makes decision based on MEASUREMENT REPORT and RRM information to hand off the UE.</u> Source: 3GPP TS 36.300 version 13.10.0 Release 13

CONFIDENTIAL

16

Claim 7	ACCUSED PRODUCTS
The mobile station apparatus according to claim 5, wherein the notification information includes at least one of an ID of mobile station apparatus, a detection result by the mobile station, and a communication state at the mobile station apparatus.	Each Accused Product is a mobile station apparatus configured to transmit notification information that includes at least one of an ID of mobile station apparatus, a detection result by the mobile station, and a communication state at the mobile station apparatus. For example, the notification information sent by the UE includes a detection result (e.g., measurement report). As shown in Fig. 2, when equation (25) holds for a given TTT then the handover can be initiated, where the <u>UE sends the measurement report to the eNB of the serving cell</u>. The serving cell starts observing the incoming consecutive time slots after TTT starts. If the RSRP difference is less than or equal to HOM in any of the incoming consecutive time slots, the HO process will be reset, otherwise, handover process will be executed. This procedure is called the HO decision. Afterward, the preparation time is modeled as a constant protocol delay “C” in a millisecond. When the preparation has been completed, the serving cell sends the HO Command message to the UE in downlink (HO Command Process) [42]–[44]. Source: Mohammed H. Hachemi et al., <i>Predicting the Probability of Spectrum Sensing with LMS Process in Heterogeneous LTE Networks</i>, Radioengineering, December 2016, at 6.

CONFIDENTIAL

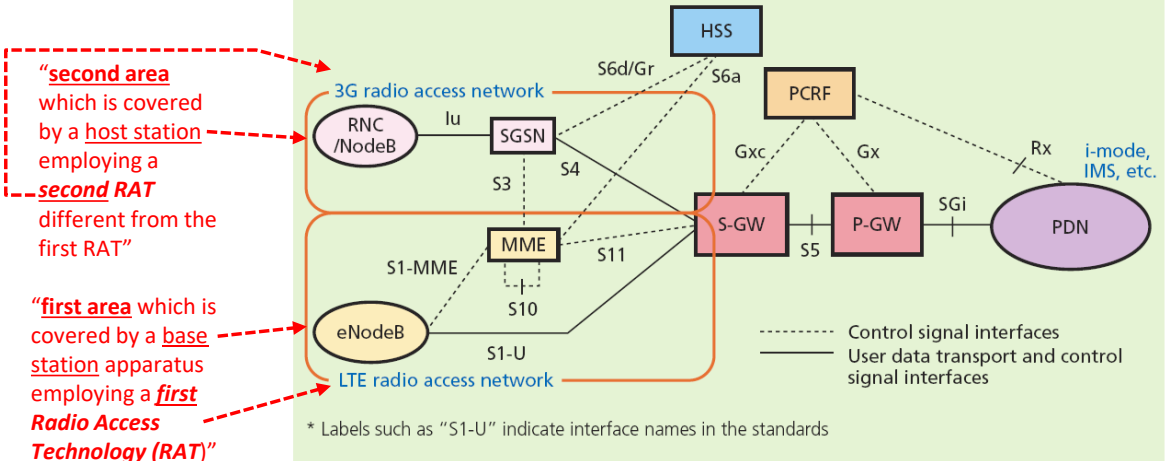
17

U.S. Patent No. 8,467,723

Claim 9	ACCUSED PRODUCTS																								
A 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, the communication method comprising:	Each Accused Product is a mobile station apparatus that performs a communication method. For example, the Accused Products include, but are not limited to the Aruba 9004-LTE Gateway. The Accused Products operate in conformance with 3GPP standards, including all versions of each standard referenced herein. Each Accused Product is User Equipment ("UE") as defined by 3GPP.  <table border="1"> <thead> <tr> <th colspan="2">Integrated LTE ^</th></tr> </thead> <tbody> <tr> <td colspan="2">AVAILABLE ON THE 9004-LTE ONLY</td></tr> <tr> <td>Downlink/Uplink Speed</td><td>600/150 Mbps</td></tr> <tr> <td>LTE Category</td><td>12</td></tr> <tr> <td>Connectors</td><td>2xSMA connectors for Main and Diversity Antenna 1xSMA connector for GPS Antenna</td></tr> <tr> <td colspan="2">BANDS SUPPORTED</td></tr> <tr> <td>Regions Supported</td><td>Global</td></tr> <tr> <td>LTE-FDD</td><td>B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20/B21/B25/B26/B28/B29/B30/B32/B66</td></tr> <tr> <td>LTE-TDD</td><td>B38/39/B40/B41</td></tr> <tr> <td>2 x CA</td><td>B1+B3/B5/B18/B19/B20/B21/B26; B2+B2/B4/B5/B12/B13/B17/B29/B30/B66; B3+B3/B5/B7/B8/B9/B20/B28; B4+B4/B5/B12/B13/B17/B25/B30; B5+B7/B25/B30/B66; B7+B7/B20/B28; B12+B25/B30; B13+B66; B20+B32; B25+B25/B26/B41; B29+B30; B38+B38; B40+B40; B41+B41; B66+B66</td></tr> <tr> <td>3 x CA</td><td>DL inter-band 3CA: B1+B3+B7; B1+B3+B19; B1+B3+B20; B1+B19+B21; B2+B4+B5; B2+B4+B13; B2+B5+B30; B2+B12+B30; B2+B29+B30; B3+B7+B20; B3+B7+B28; B4+B5+B30; B4+B12+B30; B4+B29+B30; B5+B66+B2; B13+B66+B2 DL 2 contiguous plus inter-band 3CA: B2+B2+B5; B2+B2+B13; B3+B3+B7; B3+B7+B7; B3+B3+B20; B4+B4+B5; B4+B4+B13; B5+B66+B66; B13+B66+B66; B66+B66+B2; B66+B66+B66</td></tr> <tr> <td>UMTS</td><td>B1/B2/B3/B4/B5/B8/B19</td></tr> </tbody> </table> https://www.arubanetworks.com/products/wireless/gateways-and-controllers/9000-series/	Integrated LTE ^		AVAILABLE ON THE 9004-LTE ONLY		Downlink/Uplink Speed	600/150 Mbps	LTE Category	12	Connectors	2xSMA connectors for Main and Diversity Antenna 1xSMA connector for GPS Antenna	BANDS SUPPORTED		Regions Supported	Global	LTE-FDD	B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20/B21/B25/B26/B28/B29/B30/B32/B66	LTE-TDD	B38/39/B40/B41	2 x CA	B1+B3/B5/B18/B19/B20/B21/B26; B2+B2/B4/B5/B12/B13/B17/B29/B30/B66; B3+B3/B5/B7/B8/B9/B20/B28; B4+B4/B5/B12/B13/B17/B25/B30; B5+B7/B25/B30/B66; B7+B7/B20/B28; B12+B25/B30; B13+B66; B20+B32; B25+B25/B26/B41; B29+B30; B38+B38; B40+B40; B41+B41; B66+B66	3 x CA	DL inter-band 3CA: B1+B3+B7; B1+B3+B19; B1+B3+B20; B1+B19+B21; B2+B4+B5; B2+B4+B13; B2+B5+B30; B2+B12+B30; B2+B29+B30; B3+B7+B20; B3+B7+B28; B4+B5+B30; B4+B12+B30; B4+B29+B30; B5+B66+B2; B13+B66+B2 DL 2 contiguous plus inter-band 3CA: B2+B2+B5; B2+B2+B13; B3+B3+B7; B3+B7+B7; B3+B3+B20; B4+B4+B5; B4+B4+B13; B5+B66+B66; B13+B66+B66; B66+B66+B2; B66+B66+B66	UMTS	B1/B2/B3/B4/B5/B8/B19
Integrated LTE ^																									
AVAILABLE ON THE 9004-LTE ONLY																									
Downlink/Uplink Speed	600/150 Mbps																								
LTE Category	12																								
Connectors	2xSMA connectors for Main and Diversity Antenna 1xSMA connector for GPS Antenna																								
BANDS SUPPORTED																									
Regions Supported	Global																								
LTE-FDD	B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20/B21/B25/B26/B28/B29/B30/B32/B66																								
LTE-TDD	B38/39/B40/B41																								
2 x CA	B1+B3/B5/B18/B19/B20/B21/B26; B2+B2/B4/B5/B12/B13/B17/B29/B30/B66; B3+B3/B5/B7/B8/B9/B20/B28; B4+B4/B5/B12/B13/B17/B25/B30; B5+B7/B25/B30/B66; B7+B7/B20/B28; B12+B25/B30; B13+B66; B20+B32; B25+B25/B26/B41; B29+B30; B38+B38; B40+B40; B41+B41; B66+B66																								
3 x CA	DL inter-band 3CA: B1+B3+B7; B1+B3+B19; B1+B3+B20; B1+B19+B21; B2+B4+B5; B2+B4+B13; B2+B5+B30; B2+B12+B30; B2+B29+B30; B3+B7+B20; B3+B7+B28; B4+B5+B30; B4+B12+B30; B4+B29+B30; B5+B66+B2; B13+B66+B2 DL 2 contiguous plus inter-band 3CA: B2+B2+B5; B2+B2+B13; B3+B3+B7; B3+B7+B7; B3+B3+B20; B4+B4+B5; B4+B4+B13; B5+B66+B66; B13+B66+B66; B66+B66+B2; B66+B66+B66																								
UMTS	B1/B2/B3/B4/B5/B8/B19																								

CONFIDENTIAL

18

Claim 9	ACCUSED PRODUCTS
A 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, the communication method comprising:	Each Accused Product performs a 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. For example, the Accused Products operate on LTE and other RAT systems. The Evolved Packet Core ("EPC"), the core network of the LTE system, supports multiple access technologies and allows for handover between these accesses, including accommodation of LTE and 3G as shown in the figure below. In EPC, the Serving Gateway ("S-GW") transports IP data traffic between the User Equipment ("UE") (such as the Accused Products) and the external networks and is the point of interconnect between the radio-side and the EPC. The S-GW is the anchor point for the inter-RAT mobility (such as in case of handover between LTE and other 3GPP accesses).  Figure 1 EPC network architecture Source: https://www.cultofmac.com/421369/; https://www.docomo.ne.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol11_3/vol11_3_004en.pdf

CONFIDENTIAL

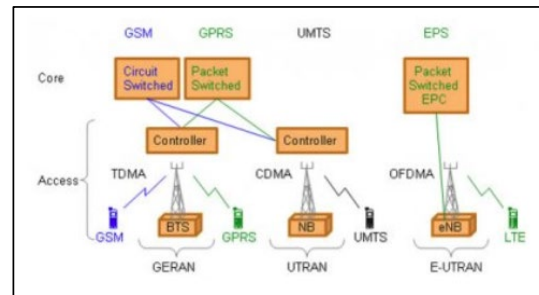
19

Claim 9

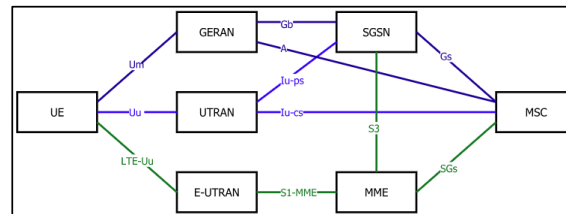
A communication method performed by a mobile station apparatus that belongs to a first area, which is covered by a base station apparatus employing a first Radio Access Technology (RAT), the first area including part or entirety of a second area which is covered by a host station employing a second RAT different from the first RAT, the communication method comprising:

ACCUSED PRODUCTS

In accordance with 3GPP specifications, the Accused Products supports inter-RAT handover of a UE between LTE radio access networks (E-UTRAN) and radio access networks using older generation radio access technologies such as UTRAN (3G), UMTS (3G GSM), GPRS (GSM 2G, 3G packet mobile data), and GERAN (3G GSM EDGE RAN). For example, the figures below depict features of the different RAN, how they coexist, and how they are arranged.

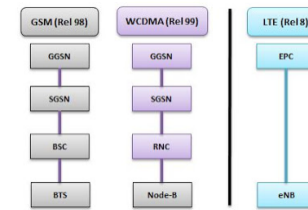


Source: <https://www.techplayon.com/lte-overview/>



Source: <https://upload.wikimedia.org/wikipedia/en/a/af/LTE-CSFB-E-UTRAN-UTRAN-GERAN-Interfaces.svg>

Below figure shows the architecture comparison of GERAN vs UTRAN vs E-UTRAN



GERAN vs UTRAN vs E-UTRAN

Design Comparison

Refer the below mentioned table for design comparison GERAN vs UTRAN vs E-UTRAN

Comparison	GERAN	UTRAN	LTE
Radio Access	FDMA/TDMA	WCDMA	OFDMA/SC-FDMA
Bandwidth	200KHz	5MHz	1.4, 3, 5, 10, 15, 20 MHz
Data Rate	14.4Kbps ~ 1.89Mbps	384Kbps ~ 42Mbps	300Mbps
Mobility (KM/Hr)	100	120	350
Latency	700 ~ 180ms	220~110ms	< 100ms for Control Plane < 5ms for Data Plane
Services	Both circuit & packet switched	Both circuit & packet switched	Packet Switched only
Architecture	4 NW nodes (not flat)	4 NW nodes (not flat)	2 NW nodes (flat)

Design Comparison

Source: <https://wirelessworld5g.com/geran-utran-comparison-with-lte/>

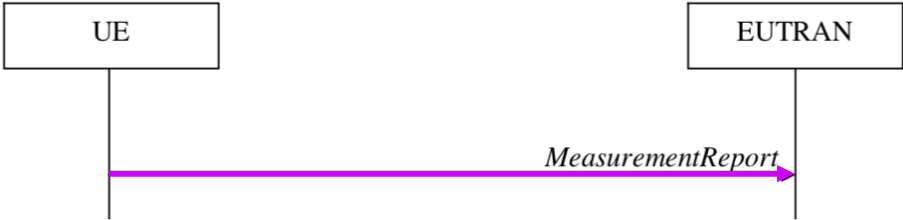
CONFIDENTIAL

Claim 9	ACCUSED PRODUCTS
A 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, the communication method comprising:	An inter-RAT handover occurs when the mobile station's radio connection is switched from the base station (e.g., LTE eNB) employing a first RAT (e.g., LTE) to a host station (e.g., RNC/NodeB) employing a second RAT (e.g., 3G). RAT handover scenarios include: (i) between E-UTRAN (LTE) and UTRAN or GERAN (both 3G) and (ii) between MTS (3G UTRAN) and GERAN (3G). <u>Inter-RAT handover</u>: indicates the transfer of the connection, under the control of the network, between the MS and two different radio access technologies (e.g. UMTS to GERAN Iu mode). Source: 3GPP TS 44.118 version 15.0.0 Release 15 5.5.2.1 <u>E-UTRAN to UTRAN Iu mode Inter RAT handover</u> 5.5.2.1.1 General 1. <u>The source eNodeB decides to initiate an Inter-RAT handover to the target access network, UTRAN Iu mode.</u> At this point both uplink and downlink user data is transmitted via the following: Bearer(s) between UE and source eNodeB, GTP tunnel(s) between source eNodeB, Serving GW and PDN GW. If the UE has an ongoing emergency bearer service the source eNodeB shall not initiate PS handover to a UTRAN cell that is not IMS voice capable. Source: 3GPP TS 23.401 version 15.6.0 Release 15 "MS" = ↑ "mobile station"

CONFIDENTIAL

Claim 9	ACCUSED PRODUCTS
A 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, the communication method comprising:	The first area includes part or entirety of a second area which is covered by a host station employing a second RAT different from the first RAT. For example, for each carrier operating in an area, the areas covered by different RAT overlap with one another according to where the carriers' eNB/NodeB/RNC are located (see below, left). For economies of scale and cost savings, many carriers deploy their eNB/NodeB/RNC from the same physical location (e.g., cell tower), thus resulting in a direct overlapping RAT area in the vicinity of the deployment (see below, right). The Accused Products are configured to operate pursuant to both of these examples. For example, cellular providers utilizes tower that employ multiple RAT, thus providing an overlapping first area for a first RAT (e.g. LTE) and second area for a second RAT (e.g. 3G). First area Second area First area Second area Source: https://www.prismatelecomtesting.com/solutions/network-equipment-manufacturers/ran-testing/inter-rat-ho-testing/ Source: https://www.netmanias.com/en/?m=view&id=blog&no=10908

CONFIDENTIAL

Claim 9	ACCUSED PRODUCTS
transmitting, 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 and	Each Accused Product transmits, to the base station apparatus, notification information while the mobile station apparatus is using the first RAT. For example, E-UTRAN UEs (such as the Accused Products) include a transmitter to transmit notification information (e.g., measurement information) to the base station apparatus (e.g., the E-UTRAN eNB) while using the first RAT (e.g., LTE). 5.5 Measurements 5.5.1 Introduction <u>The UE reports measurement information in accordance with the measurement configuration as provided by E-UTRAN.</u> E-UTRAN provides the measurement configuration applicable for a UE in RRC_CONNECTED by means of dedicated signalling, i.e. using the <i>RRCConnectionReconfiguration</i> message. Source: 3GPP TS 36.331 version 11.19.0 Release 11 5.5.5 Measurement reporting  <pre> sequenceDiagram participant UE participant EUTRAN UE->>EUTRAN: MeasurementReport </pre> Figure 5.5.5-1: Measurement reporting Source: 3GPP TS 36.331 version 11.19.0 Release 11

CONFIDENTIAL

Claim 9	ACCUSED PRODUCTS
transmitting, 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 and	Each Accused Product transmits notification information when the mobile station apparatus detects that the mobile station apparatus is located in the second area while using the first RAT. For example, in the 4G-to-3G use case, the E-UTRAN UEs report measurement information for multiple types of RAT cells according to the UE's measurement configuration. Further, when a E-UTRAN UE detects that it is located in the second area while using the first RAT (e.g., the UE is within a 3G radio cell while still connected to its LTE eNB) the UE will procure measurement data for the cells of the second area. 5.5 Measurements 5.5.1 Introduction <u>The UE reports measurement information in accordance with the measurement configuration as provided by E-UTRAN.</u> E-UTRAN provides the measurement configuration applicable for a UE in RRC_CONNECTED by means of dedicated signalling, i.e. using the <i>RRCConnectionReconfiguration</i> message. The measurement procedures <u>distinguish the following types of cells:</u> 1. <u>The serving cell(s)</u>– these are the PCell and one or more SCells, if configured for a UE supporting CA. 2. <u>Listed cells</u> - these are cells listed within the measurement object(s). 3. <u>Detected cells</u> - these are cells that are not listed within the measurement object(s) but are detected by the UE on the carrier frequency(ies) indicated by the measurement object(s). Source: 3GPP TS 36.331 version 11.19.0 Release 11

CONFIDENTIAL

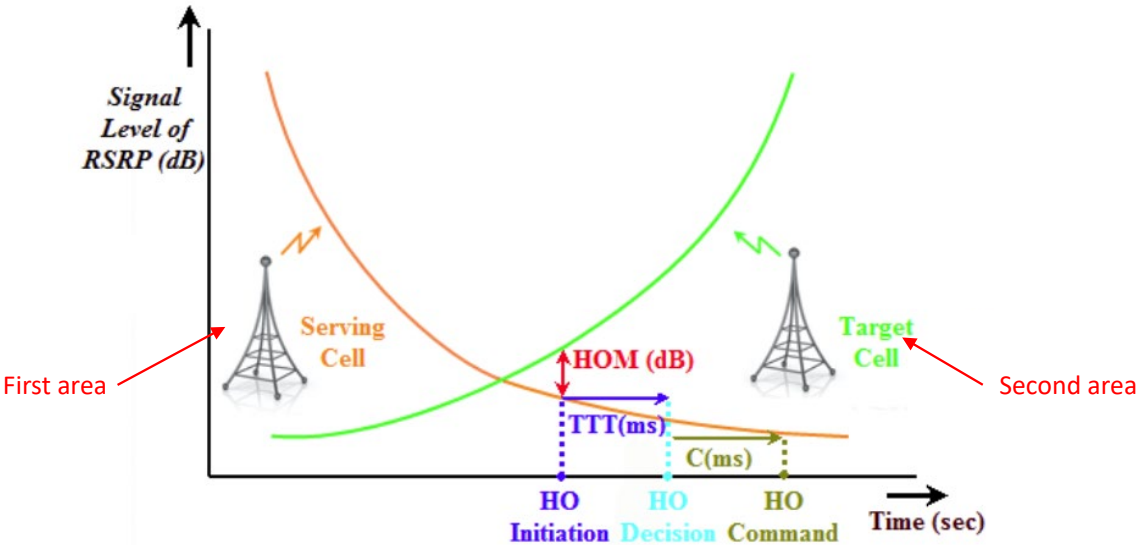
24

U.S. Patent No. 8,467,723

Claim 9	ACCUSED PRODUCTS
transmitting, 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 and	In the 4G-to-3G use case, the UE belongs to an LTE macro cell (a “first area”) covered by an LTE eNB (“a base station apparatus employing a first RAT”). As E-UTRAN UEs measure and report on multiple cells of base/host stations employing various RATs, overlap exists in base/host station cell coverage, and the first area that the E-UTRAN UE belongs to (e.g., covered by 4G LTE eNB, the “base station”) includes part or the entirety of a second area covered by a host station (e.g., a 3G NodeB or RNC). This cell coverage overlap is present during a UE inter-RAT handover. Different types of cells (e.g. serving, listed, detected, and within range) are measured and reported on under the various inter-RAT scenarios. For E-UTRA, the UE measures and reports on the serving cell(s), listed cells and detected cells. For inter-RAT UTRA, the UE measures and reports on listed cells and optionally on cells that are within a range for which reporting is allowed by E-UTRAN. For inter-RAT GERAN, the UE measures and reports on detected cells. For inter-RAT CDMA2000, the UE measures and reports on listed cells. NOTE 2: For inter-RAT UTRA and CDMA2000, the UE measures and reports also on detected cells for the purpose of SON. Source: 3GPP TS 36.331 version 11.19.0 Release 11

CONFIDENTIAL

25

Claim 9	ACCUSED PRODUCTS
transmitting, 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 and	The diagram below illustrates how a UE moving from the area of a serving cell ("first area" with eNB "base station apparatus") into a separate area covered by a target cell ("second area" with a NodeB or RNC "host station") will experience changing RF signal conditions from each cell. These changing signal conditions (i.e. the serving cell's signal becoming weaker as the target cell's signal becomes stronger) will trigger the UE handing over from the serving cell ("first area") to the target cell ("second area"). The UE is aware of the changing RF signal conditions based on its measuring the cells' RF signals.  Principle of the LTE hard handover process. Source: https://www.researchgate.net/figure/Principle-of-the-LTE-hard-handover-process_fig1_311642429

CONFIDENTIAL

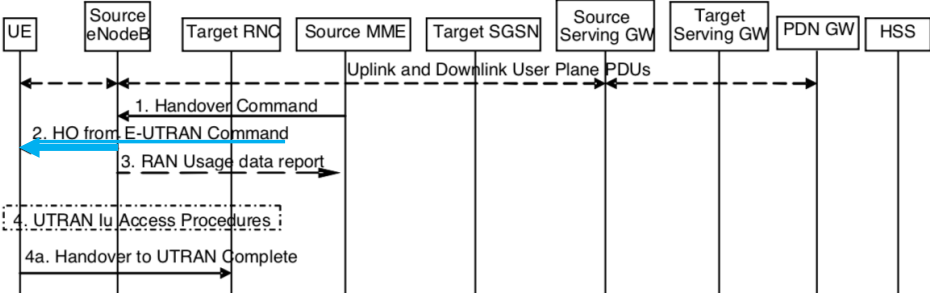
26

U.S. Patent No. 8,467,723

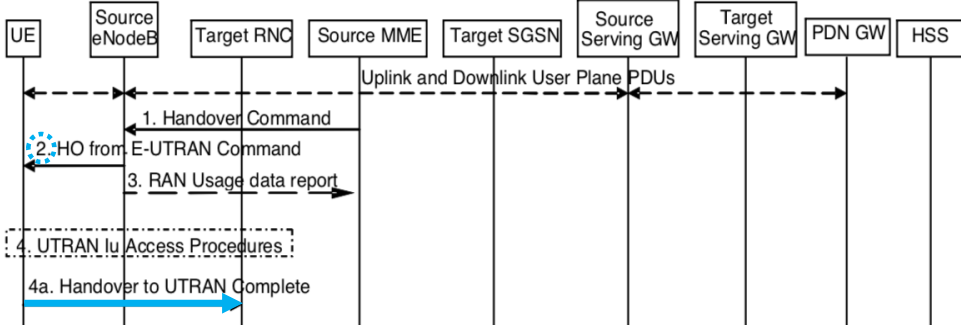
Claim 9	ACCUSED PRODUCTS
transmitting, to the base station apparatus, notification information while the mobile station apparatus is using the first RAT when the mobile station apparatus detects that the mobile station apparatus is located in the second area while using the first RAT and	The UE is aware of the changing RF signal conditions based on its measuring the cells' RF signals. The notification information is transmitted when a UE (such as an Accused Product) detects that it is located in the second area while using the first RAT. In the 4G-to-3G use case, the trigger for the E-UTRAN UE to send notification information (measurement results) to its connected eNB is based on the UE's measurement configuration, which configures the types of inter-RAT neighbor cells to measure and other variables such as thresholds and timing for measurement events. When a UE is within range (in the second area) of the inter-RAT neighbor cell, the UE will take measurements, the results of which, if meeting a configured measurement process, will trigger a handover to the inter-RAT neighbor cell. 5.5.4 <u>Measurement report triggering</u> 5.5.4.7 <u>Event B1 (Inter RAT neighbour becomes better than threshold)</u> The UE shall: 1> for UTRA and CDMA2000, only trigger the event for cells included in the corresponding measurement object; 1> consider the entering condition for this event to be satisfied when condition B1-1, as specified below, is fulfilled; 1> consider the leaving condition for this event to be satisfied when condition B1-2, as specified below, is fulfilled; <u>Inequality B1-1 (Entering condition)</u> $Mn + Ofn - Hys > Thresh$ Inequality B1-2 (Leaving condition) $Mn + Ofn + Hys < Thresh$ The variables in the formula are defined as follows: <u>Mn</u> is the measurement result of the inter-RAT neighbour cell, not taking into account any offsets. For CDMA 2000 measurement result, <i>pilotStrength</i> is divided by -2. <u>Ofn</u> is the frequency specific offset of the frequency of the inter-RAT neighbour cell (i.e. <i>offsetFreq</i> as defined within the <i>measObject</i> corresponding to the frequency of the neighbour inter-RAT cell). <u>Hys</u> is the hysteresis parameter for this event (i.e. <i>hysteresis</i> as defined within <i>reportConfigInterRAT</i> for this event). <u>Thresh</u> is the threshold parameter for this event (i.e. <i>b1-Threshold</i> as defined within <i>reportConfigInterRAT</i> for this event). For CDMA2000, <i>b1-Threshold</i> is divided by -2. Source: 3GPP TS 36.331 version 11.19.0 Release 11

CONFIDENTIAL

27

Claim 9	ACCUSED PRODUCTS
performing handover based on traffic control by the base station apparatus using the notification information.	Each Accused Product performs handover based on traffic control by the base station apparatus using the notification information. For example, in the 4G-to-3G use case, the UE's controller is responsive to a HO (handover) message received from its LTE eNB ("performing handover based on traffic control by the base station apparatus using the notification information"), based on the UE's measurement configuration and its reported measurement results. 5.5.2.1 <u>E-UTRAN to UTRAN lu mode Inter RAT handover</u> 5.5.2.1.3 <u>Execution phase</u>  2. <u>The source eNodeB will give a command to the UE to handover to the target access network via the message HO from E-UTRAN Command.</u> This message includes a transparent container including radio aspect parameters that the target RNC has set-up in the preparation phase. The details of this E-UTRAN specific signalling are described in TS 36.300 [5]. Source: 3GPP TS 23.401 version 15.6.0 Release 15

CONFIDENTIAL

Claim 9	ACCUSED PRODUCTS
performing handover based on traffic control by the base station apparatus using the notification information.	In the 4G-to-3G use case, the base station performs traffic control for the UE by sending the UE a HO message, which triggers a handover by causing the UE to detach from 4G E-UTRAN and attach to 3G (UTRAN in the diagram below) according to the parameters provided in the HO message. 5.5.2.1 E-UTRAN to UTRAN Iu mode Inter RAT handover 5.5.2.1.3 Execution phase  3GPP TS 23.401 version 15.6.0 Release 15 4. <u>The UE moves to the target UTRAN Iu (3G) system and executes the handover according to the parameters provided in the message delivered in step 2.</u> The procedure is the same as in step 6 and 8 in clause 5.2.2.2 in TS 43.129 [8] with the additional function of association of the received RABs and existing Bearer Id related to the particular NSAPI. Source: 3GPP TS 23.401 version 15.6.0 Release 15

CONFIDENTIAL

29