an ALTEN group company

Innovate, Digitize, Transform

vWLC

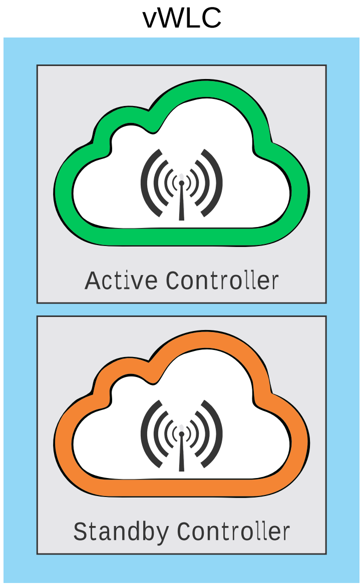
www.acldigital.com

INTRODUCTION

This document serves the purpose of describing significant aspects of the virtual WLAN controller from ACL Digital. The Cloud-based ACL Digital Wireless LAN Controller (ACL-WLC) replaces the traditional on-site dedicated WLAN controller devices. ACL-WLC Virtual Appliance is centrally deployed and managed on ACL Digital Cloud-based Network Function Virtualization services platform (NFVOps). It can be used to manage APs of not just a single site, but APs spread across geographical locations, across multiple client sites. This ensures a uniform Wi-Fi service delivery experience across all of your work locations. The distributed-forwarding aspect of our solution ensures that data is handled locally, but is managed centrally. This implies that the policies are defined centrally from the Controller's Web/Mobile App based console, but are applied locally at all the APs managed by the Controller.

OVERVIEW

ACL Digital offers a Cloud based Virtual WLAN Controller solution based on the "central control, distributed forwarding" model for lightweight management, control, and authentication of Wi-Fi services. The Cloud-based controller can manage 100s of APs. The main features of the cloud-based WLC includes:



» Remediation: vWLC has several active services running, such as WCP, Radius, DHCP, HTTP, etc which are actively monitored by NFVOps VNF Manager and remediated when service fails. If an instance totally fails, then a new instance is created by the VNF Manager.

» Auto-Scaling: This feature ensures an automated and a dynamic management of resources based on defined policies. Depending on the auto scaling policy, new instances are provisioned to handle more workload or brought down when workload is below the threshold defined in the policy.

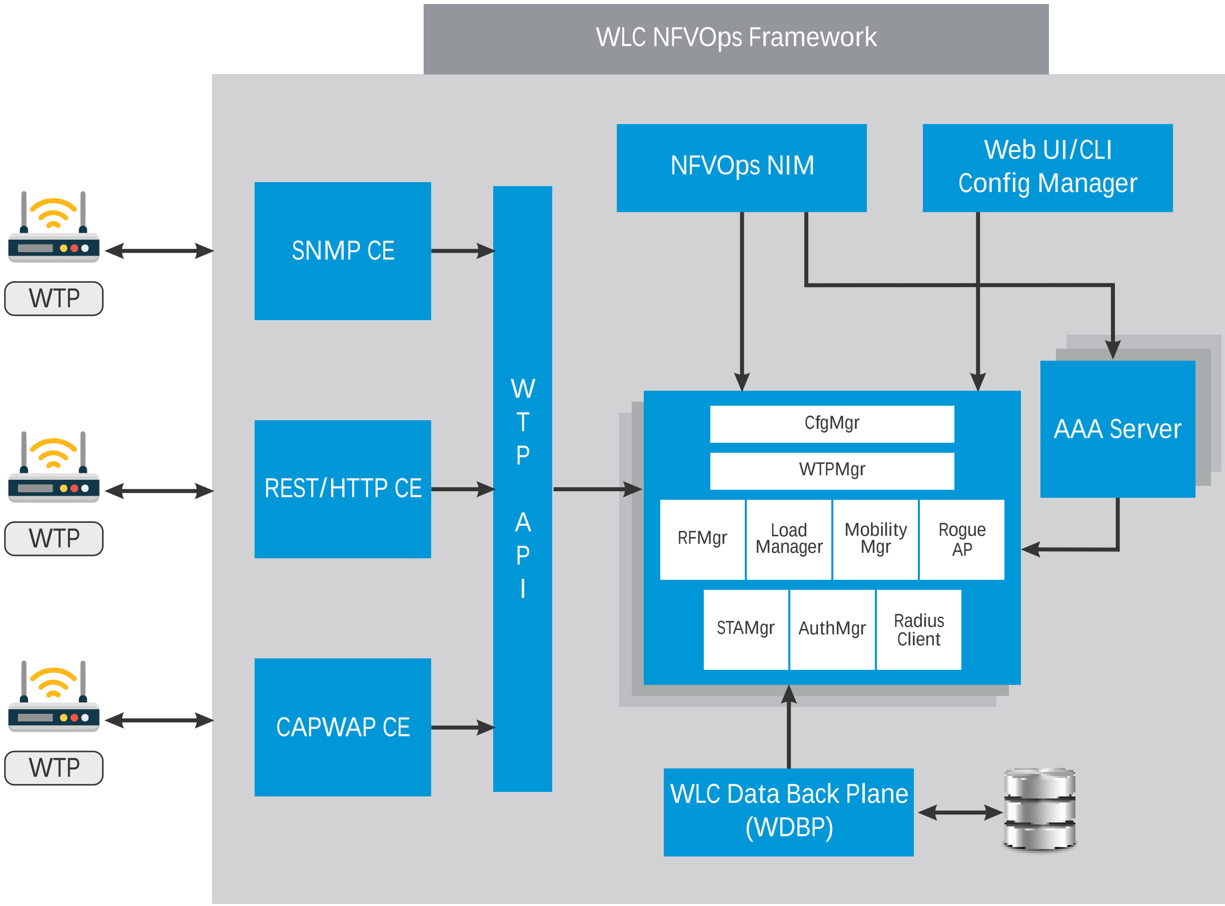
» Active-Standby Failover: When the VNF is configured for high availability, the vWLC is provisioned as a pair of two VNFs, the primary controller being on Active mode and a secondary controller will be on standby mode. When service disruption or failure occurs, the VNF Manager will switch over to standby controller and bring it to active mode. The failure will be remediated in the primary controller and it will be brought to standby mode.

» Centralized Control: The WLC provides a simple yet-powerful web and mobile based managent interface for every tenant to allow them to effectively monitor and manage their WLAN networks. The Controller can automatically manage APs using CAPWAP, ssh/cli, https,SNMP. The communication engines of the ACL-WLC take care of protocol specific communication with the APs. Once the AP starts sending shout-outs to the Controller, the ACL-WLC automatically on-boards the newly discovered AP and applies a set of pre-defined configurations on it. This plug-and-play nature of our solution makes setting up and extending the Wi-Fi network a few minutes job only.

- Centralized Client Authentication: The WLC-ACL implements the IEEE 802.11 upper MAC – this implies that all clients' state and authentication is managed at the Controller. The APs just act as a conduit forwarding all authentication requests from the clients to the WLC-ACL. The WLC-ACL takes on the 802.1x Authenticator's role. This way, it's only the controller that interacts with the centralized AAA server – instead of each AP separately talking to the AAA server. It also ensures that the Controller has the complete view of the network – it is always aware of which client is connected to which AP and can cache a client's security credentials at neighboring APs in case client roaming is anticipated.
- Distributed Forwarding: The APs once on-boarded onto the Controller start running the Wifi Services as configured by the ACL-WLC. Client data across all sites is handled locally at the APs – instead of tunneling that data all the way to the controller. This ensures that there is no single point of failure. The data handling policies (for eg, vlan assignment, firewall rules, etc) are defined at the controller, pushed to the APs and applied there. Per site there could typically be one AP which is designated as the site's gateway. An AP in the gateway role could be used for enforcing policies related to firewall, content filtering, etc.

ARCHITECTURE DIAGRAM

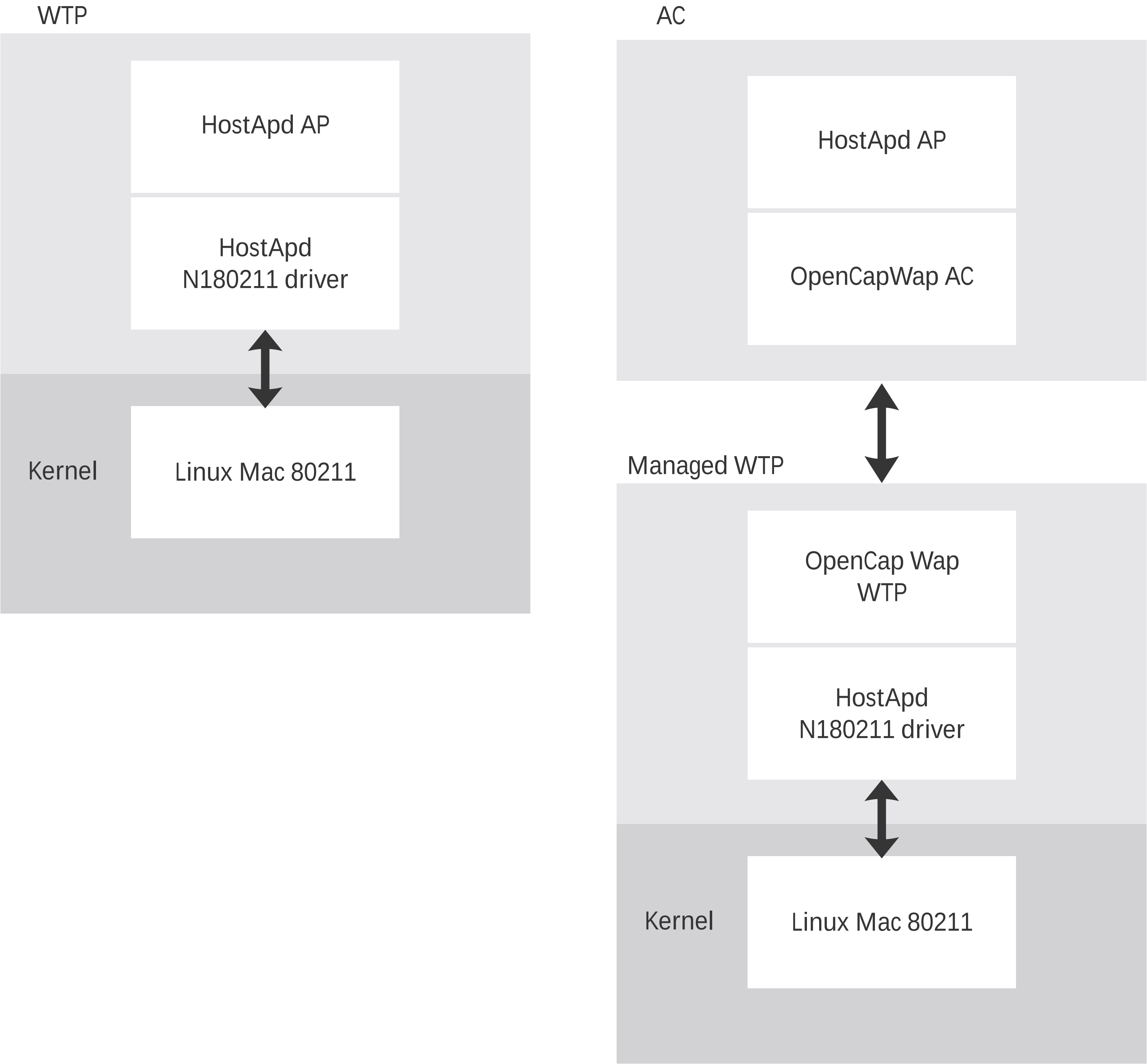
The diagram below shows vWLC as part of the overall ACL Digital NFV solution.



ACCESS CONTROLLER AND AP DETAILS

The Access Controller has been designed using the open-source components such as OpenCapwap – to provide the WTP-AC communication mechanism and HostApd, which provides the 802.11 upper Mac functionality to support Wifi client authentication and state management functionality.

The following diagram shows how OpenCapWap and HostApd have been used to convert a standalone WTP into a managed-WTP and access controller.



USE CASES

A. Subscriber Registration/ Sign-up Process

A.1 A customer who subscribes to the our WLC service shall register/sign-up him/herself on the WLC registration portal.

During the registration process, the customer shall provide the following input:

» Email id

» Password for the account

» Subscription plan: selectable from a list of options

A.2 Subscriber makes the payment for the service plan and his/her account is created

B. AP purchase and registration use-case:

B.1 The subscriber purchases the desired number of AP devices.

B.2 The subscriber signs-in to his/her account on the WLC portal.

B.3 Subscriber provides the following details for each AP purchased - The number of APs that can be registered depends on the WLC service subscription plan chosen by the customer:

B.3.1 Serial Numbers

B.3.2 MAC addresses

B.4 APs are registered

C. WLAN Service Configuration

C.1 The subscriber signs-in to his/her account on the WLC portal.

C.2 The subscriber defines the WLAN service for its WLAN network by providing the following input

C.2.1 WLAN ESSID name. This is the WLAN service name. A subscriber can define more than one WLAN service as per the subscription plan.

C.2.2 Security suite for the WLAN service. Selectable from a list of options. WPA, WPA-PSK, WPA2, WPA2-PSK, etc.

C.2.3 Provides passphrase for the WLAN service if the security type is PSK.

C.2.4 If subscribed to a AAA/Radius Service, the subscriber shall first provide a Radius server shared secret, create users and define authentication methods to be used. The subscriber shall then configure the Radius server details like server name/IP-address and shared secret on the WLAN service.

D. AP Activation

D.1 Once the subscriber plugs-in an AP in his/her premises, the AP shall start looking for the online WLC service. The URL of this WLC service shall be imprinted in every AP model supported by WLC.

D.2 The WLC service shall always keep listening for discovery messages from new APs. On discovering this AP, the WLC service shall begin the activation process.

D.3 The WLC service shall check the discovered APs' MAC/Serial-no in the list of registered APs. If the AP is registered, the WLC service shall identify the subscriber for it and will begin the AP on-boarding process.

D.4 The WLC service shall first upgrade the firmware on the newly activated AP, in case the firmware version reported by the AP is older than the latest firmware that it has.

D.5 Once the AP upgrades to the latest firmware, it will reboot and try to connect to the WLC service and steps I-IV will be performed again.

D.6 After firmware upgrade, the WLC service shall push the WLAN service configuration as defined by the Subscriber onto the AP. The AP shall apply the config and report back status.

E. Wi-Fi Client Device Activation

E.1 A client device when connecting to an AP on a subscriber's premises shall have all its connection requests forwarded by the AP to the cloud-based WLC service.

E.2 The WLC service shall authenticate the client/user as per the WLAN service configured and on-board the client.

F. AP Reports

F.1 All APs connected to the WLC service shall periodically collect data about its RF environment and report it to the WLC service. This data shall cover details about the Wi-Fi-clients and other APs in its proximity. To collect data about its neighboring APs, an AP shall run periodic background scans. The data collected shall include the BSSID/MAC of the neighboring APs, the band and channel number for each BSS, the average RSSI for each neighbor AP, etc.

G. Band Steering

G.1 In case the APs at the subscriber's premises support both 2.4Ghz and 5GHz bands, all dual-band APs will run the same WLAN service/ESSID on both the radios. If we have a client attempting to connect to this WLAN service/ESSID and it supports both 2.4GHz and 5GHz bands, in such a case if the WLC service comes to know from the RF environment data collected that there are other APs within the subscriber's premises and are within the reach of the client device, the WLC service shall reject all attempts of the client to connect to the WLAN service via the 2.4GHz radio, effectively forcing it to attempt to the same service (ESSID) on the 5GHz radio.

IMPLEMENTATION ASSUMPTIONS

Some of the assumptions behind the product are listed below.

- The vWLAN Controller solution is based on the “Centralized Control, Distributed Forwarding” architecture- implying that the Controller is the central control unit of the whole WLAN network, but all data traffic handling still happens at the individual APs. The controller implements the following 802.11 services – MIME, Authentication, De-authentication, Privacy, Association, Disassociation, and Re-association while the APs provide the distribution and integration services.

- Current version of our vWLAN Controller Framework supports many features as outlined below. Because of the addition of new features or enhancement of existing algorithms as outlined in the proposed solution for Calix, some of these features may undergo customizations:

  - Dynamic RF Management – Channel Optimization and Tx power adjustments
  - AP Load Balancing
  - Client Mobility across the ESS based on Pre-Authentication and PMK caching
  - Rogue AP Detection and Mitigation

- The following 802.11 features are currently not supported by our vWLAN Controller and support for these will have to be provided:

  - IEEE 802.11r – Fast BSS Transition
  - IEEE 802.11v – Wireless Network Management
  - IEEE 802.11k – Radio Resource Management
  - IEEE 802.11u - Interworking with External Networks