OFFICIAL RECORD DOCUMENT # 4.D-3 PRTC PROPOSAL_TAB 3 EQUIPMENT & SERVICES
PRDE-OSIATD-2018-003-WIRELESS EQUIPMENT AND SERVICES

Equipment and Service Proposal

EQUIPMENT AND SERVICE PROPOSAL

COMPANY CREDENTIALS

A strategic ally for your business

PRT is a telecommunications leader in Latin America. América Móvil is operating in 29 countries in Europe and in the region, including Mexico, Argentina, Brazil, Chile, Peru, Puerto Rico, Dominican Republic, El Salvador, Guatemala, Nicaragua, Panamá, Paraguay, Uruguay, Honduras between others. PRT offers an ample portfolio of services from the following families: Data, fixed point Internet Access, Wireless Internet, Telephone Service, Wireless Phones, Security, Data Center, and Managed Services.

This has allowed us to consolidate our position as a leader in the mobile telecommunication sector of Latin America, and as the fourth largest in the world, based on subscribers:

- More than 241 million cellular customers.
- More than 29 million telephone land lines.
- 15 million wide bandwidth accesses.
- More than 13 million subscribers of television.
- For a population of more than 940 million people.
- Offering vanguard products and quality services.

A compromise with the region, proximity to its clients and the capacity to take advantage of the opportunities that may present themselves will allow América Móvil to continue growing profitably. América Móvil is one of the three largest telecommunications companies in the world and its operations are focused on the America continent. On March of 2007, América Móvil was named by the prestigious magazine Business Week as the number one company in their classification of "Information Technology 100". This recognition was made for two years in a row. Since its formation September 2018, the Mexican company has expanded its presence with success and solidity to 25 countries of the American continent & Europe. It has driven a strong growth of subscribers and, therefore, it has penetrated in almost all countries where it is operating. This outstanding situation, has driven it to have more than 363 million cellular subscribers in the region, has implied an important compromise for investment to respond to the challenges of coverage, capacity, quality and innovation which each of the operations require.

PRT is part of América Móvil group, which manages additionally the brands Telmex and Tracfone in the United States, Embratel in Brazil, Porta in Ecuador, Telmex and Comcel in Colombia, Telmex and Telcel in México. It is the main provider of telecommunications in Puerto Rico serving over 1.8 million clients with a wide and advanced variety of services for voice, data, wide bandwidth and wireless.

Our leadership in the region is based on our experience and capacity to integrate innovative technologies which provide our clients with value added services, including various mechanisms for access and data transport.

PRT, the main provider of telecommunications in Puerto Rico, serves over 1.8 million clients with a wide and advanced variety of services for voice, data, wide bandwidth and wireless. Our constant compromise with quality and our strong service commitment allow us to build solid and lasting relationships with our clients.

America Móvil commercially launched the AMX1 submarine cable system last year and established the Cancún cable landing point. The 17,800 km submarine cable system is specifically designed for 100G transmission. Spanning over transoceanic distances, from the U.S. to Central America and Brazil, the AMX1 System will enable America Móvil to provide international connectivity to all its subsidiaries.

The cable deployment took 19 months and required overall investments of over $1.1 billion. America Móvil and Telmex will leverage the AMX1 cable system to provide voice, data and video services for their customers in Mexico and Latin America for the next 20 years.

The AMX1 System will connect seven countries with eleven landing points: Miami and Jacksonville (United States), Barranquilla and Cartagena (Colombia), Fortaleza, Salvador & Rio de Janeiro (Brazil), Puerto Plata (Dominican Republic), Cancún (Mexico), San Juan (Puerto Rico) and Puerto Barrios (Guatemala). Alcatel-Lucent has been selected for the operation and maintenance of the AMX-1 System.

AMERICA MOVIL GROUP'S MISSION STATEMENT

To consolidate ourselves as a global telecommunications group through international operations seeking to satisfy the needs and expectations in communication for our clients. We make every effort to reach the growth and financial objectives of our stockholders and contribute to the development of our human resources and well-being of the societies where our operations have a presence.

AMERICA MOVIL GROUP'S VISION

We are an enterprise group expanding and focused on internationalization, primarily in the America continent, and the integration of our businesses in the economic and technological development in telecommunications, mainly wireless, in the countries we have a presence.

WE ARE ALWAYS NEARBY, SO YOU MAY GO FARTHER

PRT is a leader in integrated communication services in Puerto Rico with almost 4,000 employees, $1.8 billion in assets and almost 2 million clients in mobile service, land lines, data transmission, Internet and television subscriptions. PRT is a subsidiary of América Móvil, S.A.B. de C.V., a leader provider in communication services in Latin America with presence in 18 countries and an impressive operational and business strength. América Móvil is the fifth business in the world in terms of the total accesses, with almost 300 million clients, and the third company of wireless services worldwide with close to 250 million subscribers.

PRT in Puerto Rico is a leader in technology with a sophisticated infrastructure 100% digital with fiber optic throughout the whole Island, and the most powerful wireless and Data network of the country with 4G coverage coast to coast and roaming in hundreds of countries around the world. With more than 5 thousand kilometers of fiber optic, our MPLS network is the strongest and more reliable Network of Puerto Rico. The company also counts with over a several modern customer service centers that are unique in the Island, and Long-Distance service, among others.

Company focus is to provide its clients with innovation, advanced technology which supports the most modern equipment, and first-class customer service with personalized attention. This has been guaranteed throughout the years with an aggressive and sustained investment plan which exceeds a billion dollars in the last 5 years and contributes in a significant way to the economic development of Puerto Rico.

PUERTO RICO NETWORK INFRASTRUCTURE

PRT is the Incumbent Local Exchange Carrier (ILEC) in Puerto Rico since 1914. PRT has focused its efforts on developing the infrastructure needed to help the citizens of PR to communicate among them, as well as with the rest of the world. As of 1997, PRT has the most complete and comprehensive telephone network and the greater variety of services on the island.

PRT has invested over $1.6 billion from 2007 to the present to expand our networks for wired and wireless access. Our switching facilities are 100% digital and consist of more than 73,000 miles of fiber optic, using SONET technology in ring configuration, with speeds of up to OC-192. This network is the main transmission medium for the public service and special facilities, and it provides more direct fiber to more business buildings than any other provider on the Island. Our cellular network positions us as the largest provider of services with island wide coverage.

It has the most advanced technology and infrastructure covering all of Puerto Rico that allows PRT to offer the most varied portfolio of technological solutions for our clients.

Our communication infrastructure is 100% digital and consists of 29 central offices and 3 offices with "Access Tandem" to insure redundancy and trust. Our network has the following characteristics:

- Approximately 80% of the transmission circuits use our fiber optic systems which consist of over 5,000 kilometers of fiber optic in ring and point to point configurations.
- The transmission networks for the metropolitan area use our fiber optic network with "Self-Healing Rings" SONET technology operating at speeds of up to OC-192, with connecting fiber at more than 200 business buildings.
- Approximately 70% of our lines composing the last mile "Local Loop" are underground.
- PRT has 4,000 employees dedicated and trained to service our client throughout the Island with presence in all the municipalities.
- Our switching and transmission networks are monitored by our Network Operating Center (NOC) 24 hours a day, 7 days a week.

WHY PRT?

PRT is the leader in numerous services and technologies because of its effective management and accelerated changes brought about in the fast-paced telecommunications field. We intend to team up and keep our leadership position, and use more effectively our human and technological resources in meeting the needs and expectations of our traditional individual and corporate clients, as well as our newest business client. The following list shows some important reasons for doing business with PRT.

- Understanding of Puerto Rico Department of Education "(PRDE)" Local and Wide Area Network needs.
- Stability – Over 99 years in Puerto Rico
- "Best of Breed" product selection
- Best project team – PRT
- Best products offer
- Full Service Organization
- Consulting Services
- Reengineering
- System and Network Integration
- Application Development
- Multivendor maintenance and support
- Provide solutions to Local, State and Federal Government Agencies

- Experience in ERATE proposal
- Financial Services
- Innovation
- Flexibility
- Quality of Service

NEW SOLUTIONS FOR YOUR COMMUNICATIONS

Our commitment with the innovation is present in each development and expressed in each service. Since the company contributes daily to the development of Puerto Rico, PRT is aware of the impact that technology has in the globalization of the economy in the present and future of businesses.

Our constant investment, advanced technology, and the commitment of the company and its employees with Puerto Rico's development make PRT the best alternative with respect to telecommunication services for all our clients.

As an enterprise and together with our business partners we are the only company which offers a total solution concept to its clients.

- DATA
  In PRT we bring data services oriented to solve the interconnection and integration of remote offices and other business sites. We have the highest trustworthiness and security of the existing technologies, thus allowing the sharing, in one same private network, all the information of your business. Thanks to our network convergence, we possess a wide capillarity which allows us to be where your business needs demand our presence.

- FIXED AND MOBILE INTERNET
  PRT's Internet services allow to have a reliable connection, fast and secure, in both wide bandwidth and dedicated access, for your office or your mobile devices - mobile phones, notebooks, tablets, etc. Our Internet backbone is the most powerful in the region and has available capacity in addition to an access network with the widest coverage, so your needs are always met.

- FIXED AND MOBILE TELEPHONE
  Our telephone solutions have been designed to satisfy the specific requirements of your business scenario. With a base on our convergence networks, we offer a wide variety of plans and maximum quality of service, considering the key factors demanded by all voice solutions: coverage, cost, functionality, scalability, quality and compatibility.

- SECURITY
  Our portfolio of advanced information security services offers the possibility of protecting the integrity, confidentiality and availability of the critical business data, by means of the technology resources managed by a team of professional experts trained under the highest worldwide standards.

- WLAN / WiFi SERVICES
  WiFi Services PRT, provides Internet connectivity to various mobile devices such as smartphones, tablets, laptops, among others; ensuring the security parameters and Superexcellent quality of services that we characterized using the most advanced technology in both centralized and locations of our customer, offering high availability of Internet service and content control using models

Our platform WiFi service, currently serves more than 800 locations island level, consolidating our position as the regional leader in WiFi service, helping our customers grow efficiently and effectively with latest technologies adapted to the needs.

- CLOUD SERVICES
  PRT Cloud facilitates the reduction of expenses related to infrastructure and its management to become an operational expense rather than a capital investment. This can be beneficial for your business both from a tax perspective, and because it allows you to conserve capital for other purposes. PRT Cloud offers a centralized, remote facility for computing, leading to economies of scale in both the use of hardware and software and a reduction in required resources for administrative management. PRT Cloud Puerto Rico makes it possible for you to access your information from anywhere at any time. While a traditional computer setup requires you to be in the same location as your data storage device, PRT Cloud takes away that step. The cloud removes the need for you to be in the same physical location as the hardware that stores your data.

- DATA CENTER SERVICES
  PRT's Data Center services, ensure maximum trustworthiness and availability for the operation of mission critical IT solutions. We have a latest-generation Data Center with the most advanced technology as far as specific infrastructure for high capacity installations.

- VIRTUAL SERVICES (IaaS)
  The virtual services also known as Virtual Machine (VM). Different from a traditional server, with this service, the client accesses, by means of a private network or via Internet, into a virtual space dedicated in the equipment located at our Data Center, having the ability of escalating immediately additional hardware or software needs to accommodate a wide variety of new applications. This product is tailored to the needs of the client under the following options: IaaS Virtual Machine Gold, Silver and Bronze.

- MANAGED SERVICES
  Our Multi services IP network and the infrastructure of the Data Center are the technological pillars of our wide portfolio of managed services. Services which allow the optimization of your investments, increase your productivity and focus on your main business skills. Based on an intelligent management of the platform, processes, improved practices worldwide and expert personnel with excellent training, we offer managed solutions for telephone over IP (unified voice mail, contact center, collaboration), Video surveillance, LAN, Information Security, Information technologies.

- OFFICE 365
  Office365 is composed of online services built on complete versions of product adapted for your consumption in mode SaaS (Software as a Service). Due to the limitations found when using a shared platform such as Office365, it is necessary to know what functionalities include the different services and how far they can be personalized.

- COLOCATION
  Installation of one or more client's server at the facilities designated by PRT. By means of a dedicated circuit or the Internet public network, the client may access their applications, in production mode or backup, without the need to acquire, maintain or renew all the elements of a Data Center, optimizing the investment in infrastructure and utilizing the resources in what really is more productive for their business.

Esm

- HOSTED IP/PBX
  Platform IP-PBX, which allows to offer unified communication functionalities and multimedia thru an IP Transport Network, which allows businesses to perform in a simple way and control their operation with immediate benefits.

- LAN / WAN / CPE / ACCESS POINTS Solutions
  PRT has business relationship and partnership with the biggest manufacturers of CPE equipment's and solutions such as Hewlett Packard Enterprise, ARUBA, Cisco, Fortinet and Avaya. We have staff with appropriate certifications for the design, configuration, deployment and monitoring of different CPE that integrate a LAN / WAN network.

EQUIPMENT PROPOSAL

New WLAN Proposed Network Design

Digital learning boost student achievements and is vital to the modernization of PRDE school curriculums. Providing a mobile-first experience ensures that the students have anytime/anywhere access for uninterrupted learning; whether it's on a school-issued device or a student' own personal device. Which means you'll need a Wi-Fi infrastructure that can support the demand of mobile devices along with the bandwidth-hungry applications running on them.

Wi-Fi-enabled Chromebooks, iPads and laptops are everywhere in the classroom. But they're only as reliable as the infrastructure they connect to. That's why it's so important to have a robust classroom wireless network that can handle every present but also future requirement.

Aruba proposed solution to PRDE new wlan includes Aruba indoor iap-305 AP's with security mountings, Aruba outdoor iap-375 AP's and Aruba Clearpass Policy Manager.

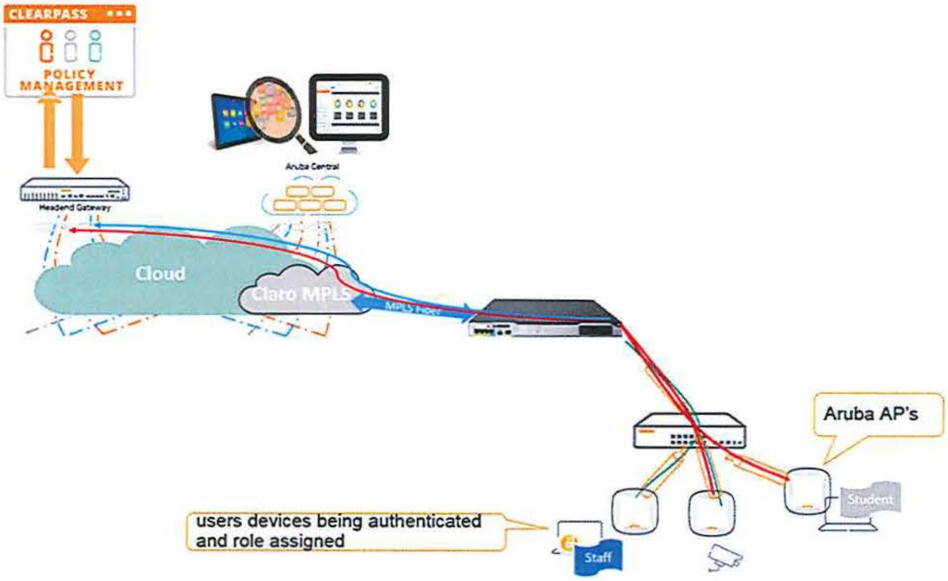
Aruba access point portfolio offers controllerless and controller-managed Wi-Fi with public cloud, private cloud and on-premises management options. PRDE will not be locked into one architecture with the proposed Aruba solution.

For the PRDE new wlan network the proposed access point will be deployed using the Aruba Instant virtual controller functionality and every access point will be managed cloud base with the Aruba Central cloud platform. The proposed solution complies and exceed all the PRDE RFP requirements. Aruba solution is the only solution that can provide investment protection and such flexibility that in the future PRDE can choose to change the architecture (on-premise controllers or on-premises management) and all the proposed access point can support either architecture.

With the Aruba instant virtual controller mode enabled a single AP automatically distributes the networks configuration to another instant AP in the same wlan layer-2 network. All these instant virtual controllers being managed cloud based with Aruba Central. This proposal assumes PoE, cabling drops and internet access availability for every AP installation. For Zero Touch Provisioning (ZTP) IP DHCP addressing also should be available.

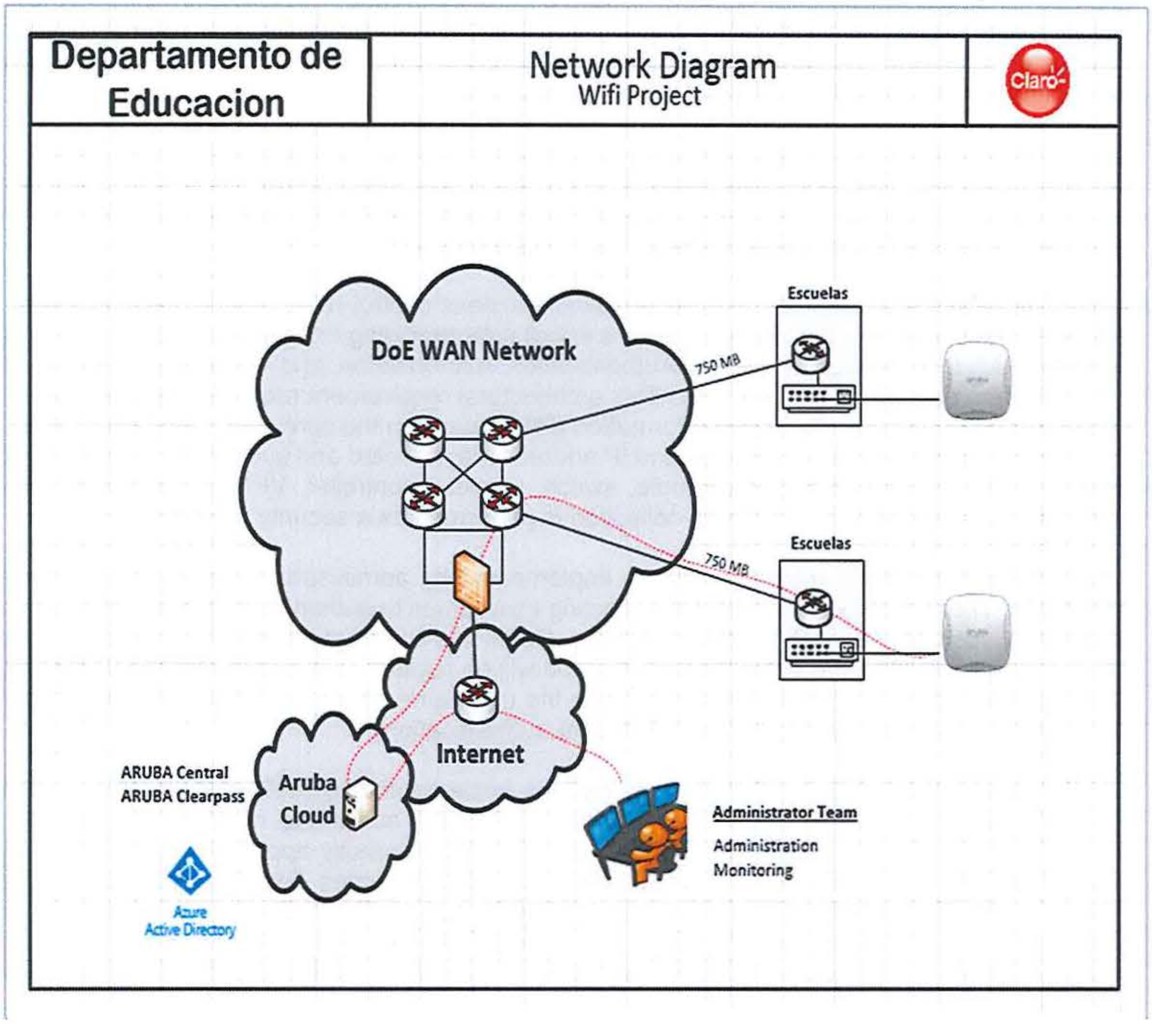
Solution Overview

Aruba's centralized architecture delivers mobility, security and convergence, leveraging a distributed deployment with centralized control. Aruba mobility controllers are software defined controllers for WLAN, LAN and WAN. They are high-performance networking platforms built specifically to run centralized ArubaOS functions such as controlled access point management, 802.11 station management, 802.11x authentication and encryption, site-to-site and client VPNs using IPsec/3DES encryption, stateful policy enforcement firewalls, L1-L7 intrusion protection, endpoint integrity checking, and seamless user roaming between access points and across mobility controllers



users devices being authenticated and role assigned

WIFI Proposal Solution Integrate to the actual DoE PR WAN



All the AP's will redirect all the authentication requests to the Aruba Clearpass Policy manager cloud deploy providing Captive Portal, Network Access Control (NAC) and AAA services including the integration with Microsoft Azure as an identity authentication source. For the required guest and student roles the solution as require will provide captive portal authentication, for the staff role the solution consider 801.1x authentication with security certificate device on-boarding.

The ClearPass Policy Manager combines all the capabilities of a robust NAC solution in one centrally managed platform. The ClearPass policy server in compliance with PRDE requirements will be deployed on the cloud, provides differentiated, context-based access control, along with operational utilities designed to reduce IT overhead for the PRDE operations team.

Aruba ClearPass is architected to provide network access control (NAC) functionality in wired, wireless, and VPN use cases. For this proposal we are specifically providing integration for the proposed new wlan network. NAC functionality is based on Authentication, Authorization, and Accounting (AAA) and is applied to any system connecting to a network. This architectural requirement requires the collection of data that is considered Personally Identifying Information (PII) to perform the core security function. At a minimum, the connecting system's MAC address and IP address are collected and audited along with the information identifying the access point (for example, switch, wireless controller, VPN concentrator, etc.) that the connection was made from. This data collection is performed as a security function.

Advanced authentication methods may be implemented by administrators to provide a higher security assurance. These methods may include collecting usernames to authenticate against local or remote user databases, such as Microsoft's Active Directory. Certificate-based authentication may also be used. The information provided by the authentication method will be audited as the user credentials for that session. Certificate-based authentications will determine the username based on the supplicant configuration. All certificate attributes are audited during certificate authentication.

Additional Advanced authorization sources may be implemented by PRDE administrators to accurately apply corporate security policy. Authentication alone does not entitle network access, only that the credentials are valid. Authorization must then be applied to correctly apply security policy. Authorization sources may be the local database or external information sources. External information sources may include Active Directory group membership, employee type (contractor, visitor, or employee), attributes obtained from configuration management servers, corporate databases, etc. The information is then used to provide appropriate access. All information used to determine access is audited with the authorization message.

The Aruba solution proposed architecture without doubt is the most cost-effective and feature rich available in the market.

Every proposed AP include a policy enforcement firewall that provide context-based controls to enforce application-layer security and prioritization. AppRF is a Deep Packet Inspection (DPI) feature that is designed to provide user-level awareness of all traffic across the network.

The proposed design will provide during the network sign-on process, the identity and role of each user or device is learned. Based on the three (3) main profiles the RFP document require, Staff and other authorized internal users like students or guest can be treated as a single class or further subdivided according to information found in a directory server. Once the role of the user or device is determined, policies are applied based on a series of administrator-defined templates. These policies follow the user throughout the WiFi network and are applied uniformly across. Aruba Clearpass Policy manager also support wired and VPN connections so in the future PRDE can consider expanding this NAC context policy into the wired school network. bandwidth-hungry protocols such as mDNS, ARP and NetBIOS broadcasts can be completely filtered and confined only to specific portions of the network.

Guest & Students Roles

For the required guest and student roles the solution proposes captive portal authentication using Microsoft Azure as identity authentication source. Clearpass can use almost any other identity authentication source like LDAP or RADIUS even simultaneously joining to more than one domain. Clearpass Policy manager can provide even self-registration for guest with their own devices, activity tracking for compliance and auditing, and unique features such as advertising and commercial-grade hotspot services.

Clearpass Auto-Adjust Captive Portal

Customizable login pages provide the ability to display the latest PRDE messaging. The ability to display separate captive portals where multiple regions, or entities exist is also supported. Data entry field customization allows for capturing additional information about guests, support for rotating background images and a variety of built-in remediation pages allow full portal customization for a variety themes and uses. Acceptance of Use acknowledgement is also supported.

Staff Roles

For the staff role, the design proposes 802.1x authentication with ClearPass Policy Manager, that automates device onboarding of personal devices via a built-in portal workflow. The onboarding portal offers full self-service configuration for Windows, Mac OS X, iOS, Android and Chrome devices. That includes the configuration of 802.1X settings as well as the distribution of unique device credentials.

This provides an incredibly simple way to configure wireless settings, apply unique per device certificates and profiles and ensure that users can securely connect their devices to 802.1X-enabled new Wi-Fi network with minimal PRDE IT interaction. With the industry's most advanced auto-provisioning features, onboarding thousands of devices is amazingly simple via integrated policy management, customizable user-facing portal and built-in certificate authority (CA).

Because the current wired Local Area Network in the schools are not segmented into VLAN's, do not have any QoS configured either have any central management school flat wired networks is a very "hostile" environment.

PRT/Claro is the current provider of the E-Rate WLAN Managed Networks. For this WLAN managed networks, we create a parallel wired Local Area Networks with multiple vlan's configured, QoS and fully managed. PRT/Claro can consider the design possibility to take advantage of some of that robust designed infrastructure, vlan segmentation and others to integrate the new WiFi network. This integration will result in the best responsible cost-efficient use of federal funding. No other proposal can offer an approach that could show an exemplary and responsible decision criteria.

Aruba AP's can be configured as DHCP servers for the wireless clients or as DHCP relay into the local area network. Can assign traffic into multiple vlan's per role or per ssid, local IDS capability, even providing content filtering directly on the AP's.

Em

Aruba Central cloud platform can retain log data for 1 year, also any other type of system data (configurations, clients connected, device count etc.) can be exported and externally storage thru the Central Platform Application Programming Interface (API's). The API Gateway feature in Central supports the REST API for all Central services. This feature allows Central users to write custom applications, embed, or integrate the APIs with their own applications. Central allows you to integrate Webhook with other third-party applications such as ServiceNOW, Zapier, IFTTT, and so on. Webhook is available as a notification option for alerts. Also available ClearPass Insight, is an advanced application included with the ClearPass Policy Manager platform to deliver enhanced analytics, in-depth reporting, and significant gains when addressing compliance and regulatory overhead.

Insight uses a powerful analytics engine that mines network access logs to generate trending report on various parameters. Network managers can utilize these trends to get an overview of authentication and access activity, elaborate client access distribution, load-averages, and analyze authentication traffic flow through various network devices.

No other vendor can offer this flexibility, needed to ensure the success of this implementation.

Proposed Aruba Campus Access Points

Aruba's portfolio of 802.11ax (Wi-Fi 6) and 802.11ac (Wi-Fi 5) access points address today's most challenging Wi-Fi use cases. Flexible deployment options allow the APs to be deployed in controller-managed, controller less (Instant), or remote access modes for midsize and large enterprise environments like the one proposed to the PRDE.

Unique in the industry, the Aruba APs are powered by ClientMatch technology — making sure all devices have the fastest connection always and Multi-User MIMO capable devices can make use of the technology. They come with an integrated Bluetooth Low Energy (BLE) beacon to help remotely manage battery-powered Aruba Beacons.

Indoor Aruba 305 Proposed Access Point

The proposed Aruba 300 Series Wave 2 access points comply and exceed PRDE requirement's delivering high performance and superb user experience for the PRDE network. These Wave 2 access points deliver multi-user MIMO (MU-MIMO) aware ClientMatch to boost network efficiency and support the growing device density demands on your network. The 305 Series also has an integrated Bluetooth Aruba Beacon that simplifies the remote management of a network of large-scale battery-powered Aruba beacons while also providing with the same AP infrastructure an optional solution for advanced location and indoor way finding, and proximity-based push notification capabilities

Aruba 305 with Security Mounting

The proposal includes the AP-200-MNT-W3 Security mount kit that offers a secure mounting solution for 300 Series access points. This mount kit can be installed onto a flat surface, or mounted onto a standard single or dual gang wall box, and includes a security screw that may be used to lock the access point to the mount for additional security.

Unique Benefits

Dual Radio 802.11ac access point with Multi-User MIMO

- Supports up to 1,300 Mbps in the 5 GHz band (with 3SS/VHT80 clients) and up to 300 Mbps in the 2.4 GHz band (with 2SS/HT40 clients) Built-in Bluetooth Low-Energy (BLE) radio
- Enables location-based services with BLE-enabled mobile devices receiving signals from multiple Aruba Beacons at the same time
- Enables management of your deployment of battery-powered Aruba Beacons Advanced Cellular Coexistence (ACC)
- Minimizes interference from 3G/4G cellular networks, distributed antenna systems and commercial small cell/femtocell equipment. Quality of service for unified communication apps Quality of service for app visibility and control
- Supports priority handling and policy enforcement for unified communication apps, including Microsoft Skype for Business with encrypted videoconferencing, voice, chat and desktop sharingmRF Management
- Adaptive Radio Management (ARM) technology automatically assigns channel and power settings, provides airtime fairness, and ensures that APs stay clear of all sources of RF interference to deliver reliable, high-performance WLANs
- The Aruba 300 Series APs can be configured to provide part-time or dedicated air monitoring for spectrum analysis and wireless intrusion protection, VPN tunnels to extend remote locations to

corporate resources, and wireless mesh connections where Ethernet drops are not available Intelligent app visibility and control.

- AppRF technology leverages deep packet inspection to classify and block, prioritize or limit bandwidth for over 2,500 enterprise apps or groups of apps Security
- Integrated wireless intrusion protection offers threat protection and mitigation, and eliminates the need for separate RF sensors and security appliances
- IP reputation and security services identify, classify, and block malicious files, URLs and IPs, providing comprehensive protection against advanced online threats
- Integrated Trusted Platform Module (TPM) for secure storage of credentials and keys Intelligent Power Monitoring (IPM)
- Enables the AP to continuously monitor and report its actual power consumption and optionally make autonomous decisions to disable certain capabilities
- For the 300 Series APs, the IPM power-save feature applies when the unit is powered by an 802.3af PoE source. By default, the USB interface will be the first feature to turn off if AP power consumption exceeds the available power budget. In rare cases it may be necessary to take additional power saving measures, but in most cases, the 300 Series APs will operate in unrestricted mode

Choose Your Operating Mode

The Aruba 300 Series APs offer a choice of operating modes to meet any present and future PRDE management and deployment requirements:

- Controller-managed mode – When managed by Aruba Mobility Controllers, Aruba 300 Series APs offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding
- Aruba Instant mode – In Aruba Instant mode, a single AP automatically distributes the network configuration to other Instant APs in the WLAN. Simply power-up one Instant AP, configure it over the air, and plug in the other APs – the entire process takes about five minutes. If WLAN requirements change, a built-in migration path allows 300 Series Instant APs to become part of a WLAN that is managed by a Mobility Controller
- Remote AP (RAP) for branch deployments
- Air monitor (AM) for wireless IDS, rogue detection and containment
- Spectrum analyzer, dedicated or hybrid, for identifying sources of RF interference
- Secure enterprise mesh

For large installations across multiple sites, the Aruba Activate service significantly reduces deployment time by automating device provisioning, firmware upgrades, and inventory management. With Aruba Activate, the Instant APs are factory-shipped to any site and configure themselves when powered up.

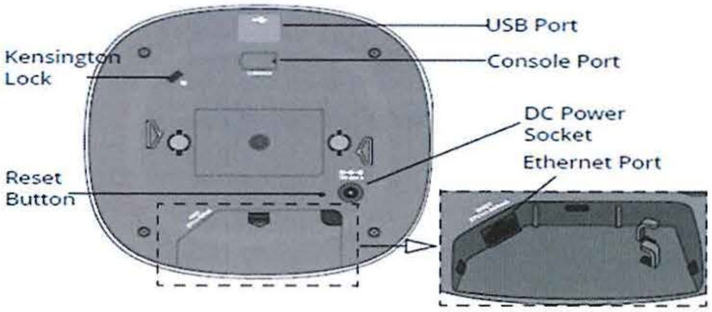
Wi-Fi Antennas

AP-304/IAP-304: Three RP-SMA connectors for external dual band antennas. Worst-case internal loss between radio interface and external antenna connectors (due to duplexing circuitry): 0.8dB in 2.4GHz and 1.6dB in 5GHz.

AP-305/IAP-305: Three integrated dual-band down tilt omni-directional antennas for 3x3 MIMO with maximum antenna gain of 3.9dBi in 2.4GHz and 5.4dBi in 5GHz. Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The down tilt angle for maximum gain is roughly 30 degrees.

- The maximum gain of the combined (summed) antenna patterns for all elements operating in the same band is 5.4dBi in 2.4GHz and 7.6dBi in 5GH

Aruba 305 AP Detail



Other Interfaces

One 10/100/1000BASE-T Ethernet network interface (RJ-45)
- Auto-sensing link speed and MDI/MDX
- 802.3az Energy Efficient Ethernet (EEE)

USB 2.0 host interface (Type A connector)
Bluetooth Low Energy (BLE) radio
- Up to 3dBm transmit power (class 2) and -92dBm receive sensitivity
- Integrated antenna with roughly 30 degrees down tilt and peak gain of 2.3dBi (AP-304/IAP-304) or 3.4dBi (AP-305/IAP-305)

Visual indicators (multi-color LEDs): for System and Radio status
Reset button: factory reset (during device power up)
Serial console interface (proprietary; optional adapter cable available)
Kensington security slot

Environmental

Operating:
- Temperature: 0° C to +50° C (+32° F to +122° F)
- Humidity: 5% to 93% non-condensing

Storage and transportation:
- Temperature: -40° C to +70° C (-40° F to +158° F)

Regulatory

FCC/Industry of Canada
CE Marked
R&TTE Directive 1995/5/EC
Low Voltage Directive 72/23/EEC
EN 300 328
EN 301 489
EN 301 893
UL/IEC/EN 60950
EN 60601-1-1 and EN 60601-1-2

Reliability

MTBF: 1,116,000hrs (127yrs) at +25C operating temperature

Ewm

Certifications

CB Scheme Safety, cTUVus
UL2043 plenum rating
Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac

For additional reference information please refer to Appendix A

Outdoor Aruba 375 Proposed Access Point

Weatherproof and temperature hardened, Aruba 370 series access points deliver 802.11ac Wave 2 Gigabit Wi-Fi to outdoor and environmentally challenging locations. Delivers 4x4:4SS MU-MIMO capability, Aruba's advanced ClientMatch and an integrated Bluetooth beacon to enable Aruba location services. Puerto Rico recent experience withstanding two hurricanes within two weeks between each other offer the opportunity to emphasize the need to strengthen our critical infrastructure that includes our telecommunications infrastructure. Aruba proposed outdoor AP's offer rugged physical capabilities like salt tolerance for coastal environments, wind survival up to 165 mph and complete waterproof construction of the AP. All these critical capabilities in addition to the software features described are industry leading and offer Puerto Rico Department of Education the infrastructure resiliency that the US Federal Government and Puerto Rico Government have described must be the goal present over every infrastructure re-build initiative.

Aruba 375 Outdoor

Unique Benefits

Dual Radio 802.11ac access point with Multi-User MIMO

- Supports up to 1,733 Mbps in the 5 GHz band (with 4SS/VHT80 or 2SS/VHT160 clients) and up to 300 Mbps in the 2.4 GHz band (with 2SS/HT40 clients). Built-in Bluetooth Low-Energy (BLE) radio
- Enables location-based services with BLE-enabled mobile devices receiving signals from multiple Aruba Beacons at the same time. Advanced Cellular Coexistence (ACC)
- Minimizes interference from 3G/4G cellular networks, distributed antenna systems, and commercial small cell/femtocell equipment. Industrial design for harsh indoor and outdoor environments
- Sealed connector interfaces to lock out dust and moisture Quality of service for unified communication apps
- Supports priority handling and policy enforcement for unified communication apps, including Microsoft Skype for Business with encrypted videoconferencing, voice, chat, and desktop sharing. Best-in-class RF management

Eom

- Integrated AirMatch technology manages the 2.4-GHz and 5-GHz radio bands and actively optimizes the RF environment including channel width, channel selection and transmit power. Spectrum analysis
- Capable of part-time or dedicated air monitoring, the spectrum analyzer remotely scans the 2.4-GHz and 5-GHz radio bands to identify sources of RF interference. Wireless mesh
- Wireless mesh connections are convenient where Ethernet drops are not available. Intelligent app visibility and control
- AppRF technology leverages deep packet inspection to classify and block, prioritize or limit bandwidth for 1,000's of enterprise apps or groups of apps. Aruba Secure Core
- Device assurance: Use of Trusted Platform Module (TPM) for secure storage of credentials and keys as well as secure boot
- Integrated wireless intrusion protection offers threat protection and mitigation and eliminates the need for separate RF sensors and security appliances.
- IP reputation and security services identify, classify, and block malicious files, URL and IPs, providing comprehensive protection against advanced online threats.
- Encrypted IPsec VPN tunnels securely connect remote users to corporate network resources.

Choose Your Operating Mode

As unified APs, the Aruba 370 Series can be deployed with or without a controller and can be readily switched to accommodate changing network needs.

- Controller mode: When managed by Aruba Mobility Controllers, Aruba 370 Series APs offer centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding or,
- Controller less (Instant) mode: In Aruba Instant mode, a single AP automatically distributes the network configuration to other Instant APs in the WLAN. Simply power-up one Instant AP, configure it over the air, and plug in the other APs – Instant Network.

Other functional modes include:

- Remote AP (RAP) mode for branch deployments
- Air monitor (AM) for wireless IDS, rogue detection and containment
- Spectrum analyzer, dedicated or hybrid, for identifying sources of RF interference
- Secure enterprise mesh
- Hybrid AP serves Wi-Fi clients and provides wireless intrusion protection and spectrum analysis

For large installations across multiple sites, the Aruba Activate service significantly reduces deployment time by automating device provisioning, firmware upgrades, and inventory management. With Aruba Activate, Unified APs are factory-shipped to any site and configure themselves when powered up.

AP-370 Series Specifications

AP-374

- 5 GHz 802.11ac 4x4 MU-MIMO (1,733 Mbps max rate)
  - Four Nf connectors for external antenna operation
- 2.4 GHz 802.11n 2x2 MIMO (300 Mbps max rate) radios
  - Two Nf connectors for external antenna operation at 2.4 GHz

AP-375

- 5 GHz 802.11ac 4x4 MU-MIMO (1,733 Mbps max rate)
  - Internal Omni Antennas 4.6 dBi
- 2.4 GHz 802.11n 2x2 MIMO (300 Mbps max rate) radios
  - Internal Omni Antennas 4.0 dBi

AP-377

- 5 GHz 802.11ac 4x4 MU-MIMO (1,733 Mbps max rate)
  - Internal 80°H x 80°V Directional Antennas 6.3 dBi
- 2.4 GHz 802.11n 2x2 MIMO (300 Mbps max rate) radios
  - Internal 80°H x 80°V Directional Antennas 6.4 dBi

Other Interfaces

One 10/100/1000BASE-T Ethernet network interfaces (RJ-45)

- Auto-sensing link speed and MDI/MDX
- 802.3az Energy Efficient Ethernet (EEE)

One 1000BASE-X SFP Port

Bluetooth Low Energy (BLE) radio

- Up to 4 dBm transmit power (class 2) and -91 dBm receive sensitivity

Visual indicator (multi-color LED): For system and radio status

Reset button: Factory reset (during device power up)

Micro USB console interface

Kensington security slot

Environmental

Operating:

- Temperature: -40° C to +65° C (-40° F to +149° F)
- Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

Operating Altitude: 3,000 m

Water and Dust

- IP66/67

Salt Tolerance

- Tested to ASTM B117-07A Salt Spray 200hrs

Wind Survival: Up to 165 Mph

Shock and Vibration ETSI 300-19-2-4

Em

Regulatory

FCC/ISED

CE Marked

RED Directive 2014/53/EU

EMC Directive 2014/30/EU

Low Voltage Directive 2014/35/EU

UL/IEC/EN 60950

EN 60601-1-1, EN60601-1-2

Certifications

CB Scheme Safety, cTUVus

UL2043 plenum rating

Wi-Fi Alliance certified 802.11a/b/g/n

Wi-Fi CERTIFIED™ ac (with wave 2 features)

For additional reference information please refer to Appendix A.

Aruba Clearpass Policy Manager

The ClearPass Policy Manager combines all the capabilities of a robust NAC solution in one centrally managed platform. The ClearPass policy server provides differentiated, context-based access control for users connected in the proposed WiFi network along with operational utilities designed to reduce IT overhead. Security starts with visibility of all devices – you can't secure what you can't see. The ClearPass Policy Manager solution provides built-in device profiling, a web-based administrative interface and comprehensive

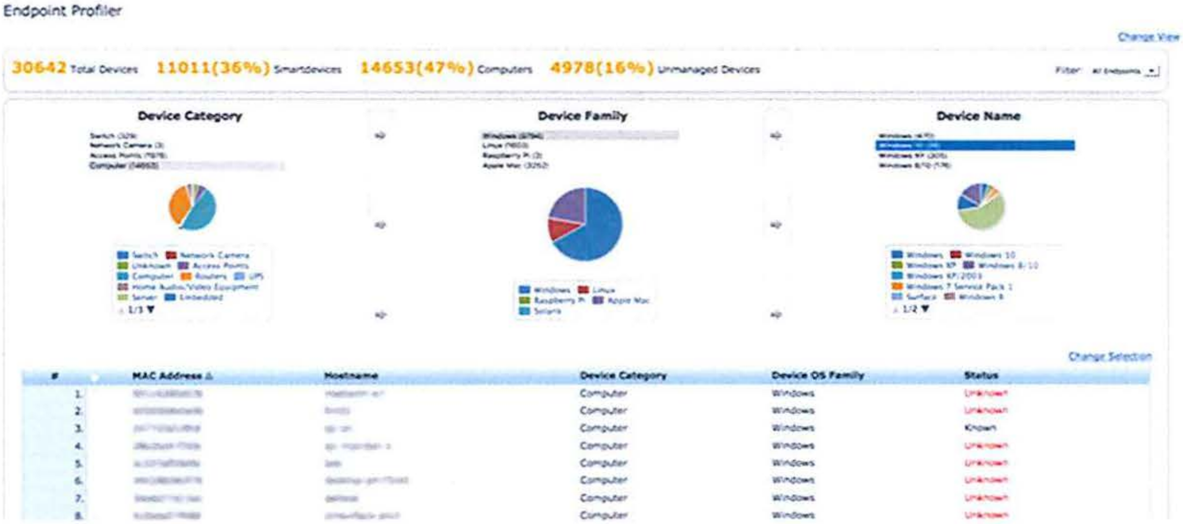
reporting with real-time alerts. All contextual data collected is leveraged to ensure that users and devices are granted appropriate access privileges – regardless of access method or device ownership.

The built-in profiling engine collects real-time data that includes device categories, vendors, OS versions, and more. There's no longer a reason to guess how many devices are connected on wired and wireless networks. Granular visibility provides the data required to pass audits and determine where performance and security risks could come from.

With ClearPass Policy Manager, PRDE in the future can easily automate and extend authentication and authorization policies across the entire organization for wireless, wired, VPN and guest access applications. Differentiated access capabilities based on a variety of attributes, including user role, device, time, and location are available.

In addition to its integrated policy management engine, and RADIUS/TACACS+ servers for AAA support, the ClearPass Policy Manager can read from multiple identity stores and databases, including those based on Microsoft Active Directory, LDAP, SQL and Kerberos. This provides a unified policy model that ensures access controls are applied consistently across the organization.

Aruba ClearPass Profiler Screen



Endpoint Profiler

Change View

30642 Total Devices 11011(36%) Smartdevices 14653(47%) Computers 4978(16%) Unmanaged Devices

Filter: All Endpoints

Change Selection

#	MAC Address	Hostname	Device Category	Device OS Family	Status
1.	[redacted]	[redacted]	Computer	Windows	Unknown
2.	[redacted]	[redacted]	Computer	Windows	Unknown
3.	[redacted]	[redacted]	Computer	Windows	Known
4.	[redacted]	[redacted]	Computer	Windows	Unknown
5.	[redacted]	[redacted]	Computer	Windows	Unknown
6.	[redacted]	[redacted]	Computer	Windows	Unknown
7.	[redacted]	[redacted]	Computer	Windows	Unknown
8.	[redacted]	[redacted]	Computer	Windows	Unknown

In addition to allowing staff employees and guests to self-register their own devices, ClearPass supports role-based access controls specific to the guest network, activity tracking for compliance and auditing, and unique features such as advertising and commercial-grade hotspot services.

Multiple guest/staff/student's portals can be used to across large organizations to segment and manage traffic across departments, brands, and locations. Social logins are supported for retail, and large public venues.

In addition, ClearPass API's, syslog messaging and Extensions capability makes it easy to exchange endpoint attributes with firewalls, SIEM, endpoint compliance suites and other solutions for enhanced policy management. These solutions can ingest endpoint attributes to match traffic patterns, per their specific rules for each device category, to optimize connections or remediate suspect traffic.

Considering the original intention of the PRDE to implement Network Access Control policies that include WiFi and wired users on every school. The Aruba solution offer the most flexible platform to achieve that goal in the future. An example of an Aruba integration that in the future can offer a vulnerability analytics engine, to scans users' device for known vulnerabilities, misconfigurations and malware is with Tenable.sc.

Tenable.sc (formerly Security Center) by Cybersecurity Industry Leader Tenable Inc., is a platform that provides a comprehensive and integrated view of enterprise security posture to reduce business risk and ensure compliance. Tenable.sc evaluates vulnerability data gathered across multiple Tenable's Nessus® scanners distributed across your enterprise, illustrates vulnerability trends over time and assesses risk to prioritize remediation and mitigation tasks.

The Extension integrates with Tenable.sc system, allowing API access to threat and vulnerability attributes obtained from scan results. This allows the Extension to provide the following integration capabilities.

1. Periodic Poll: enable periodic polling of scanned results for endpoints in Tenable.sc with a valid mac address. This allows Policy Manager to access a number of endpoint attributes which can be leveraged for creating policies.

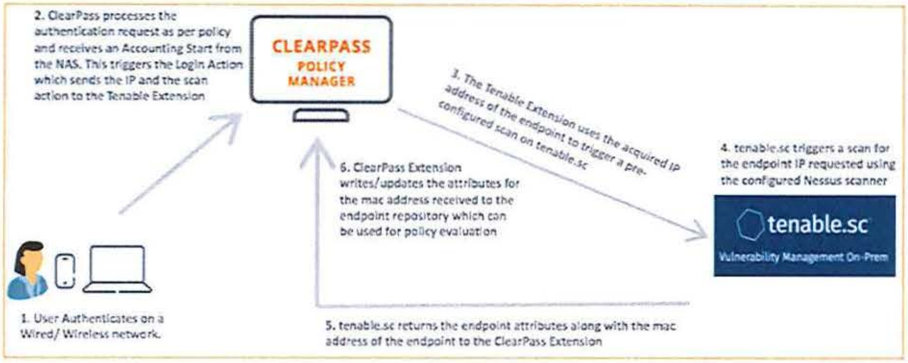
   For example:

   a) Check if the endpoint is known to Tenable's Nessus scanners
   b) Check if the Last Scan time was less than 7 days.
   c) Check if the endpoint has any Critical weaknesses.

2. Trigger a Scan: allows the Extension to trigger a configured scan on Tenable.sc for noncompliant endpoints. The scan results are sent to ClearPass Policy Manager to update the attributes in the endpoint database which can be leveraged for defining policies.

3. Authorization source (optional): trigger the Extension to get the latest posture results or attributes for the authenticated endpoint.

The diagram below shows a pictorial overview of the components and how they interact with each other:


2. ClearPass processes the authentication request as per policy and receives an Accounting Start from the NAS. This triggers the Login Action which sends the IP and the scan action to the Tenable Extension
CLEARPASS
POLICY
MANAGER
3. The Tenable Extension uses the acquired IP address of the endpoint to trigger a pre-configured scan on tenable.sc
4. tenable.sc triggers a scan for the endpoint IP requested using the configured Nessus scanner
tenable.sc
Vulnerability Management On-Prem
6. ClearPass Extension writes/updates the attributes for the mac address received to the endpoint repository which can be used for policy evaluation
1. User Authenticates on a Wired/ Wireless network.
5. tenable.sc returns the endpoint attributes along with the mac address of the endpoint to the ClearPass Extension

In addition to utilizing this information in Aruba' Clear policy Manager; with Tenable.sc you will be able to manage and measure your end users' cyber risk (extensible to other IT components). Tenable.sc does this through advanced analytics, customizable dashboards/reports and workflows.

Additional integration is available via ClearPass Exchange API's program. No other solution offers the broad solution integration options as Aruba Networks provides. Capabilities that clearly stablish Aruba as the solution that can show optimal federal funding thru the best cost effective and flexible solution in the market.

Ewm

Aruba Instant OS

Introduction

The included Aruba Instant functionality is without a doubt the single most relevant architectural advantage for the PRDE WiFi network. Consequently, PRDE or any enterprise organization need a mobility solution that's simple to set up, highly reliable, and can be managed centrally. But they also need enterprise-grade WLAN functionality.

Aruba Instant functionality uses innovative Virtual Controller technology to deliver enterprise-grade WLAN capabilities — including robust security, performance, and scalability.

Designed for ease of use, Aruba Instant can be set up in minutes with minimal IT assistance and managed centrally through Aruba Central cloud platform.

Aruba Instant Virtual Controller Overview

Aruba Instant is the only controller-less Wi-Fi solution that delivers superior Wi-Fi performance, business-grade security, resiliency and flexibility with the simplicity of zero-touch deployment being managed by Aruba Central Cloud platform. Aruba Instant is simple to setup and does not require network expertise to deploy and manage.

How it works, one dynamically-elected Instant AP automatically distributes the network configuration to other Instant APs in the network. Simply power-up one Instant AP, configure it over the air or in the cloud, and plug in the other APs – the entire process takes about five minutes.

The free local management interface, unique to Aruba Instant APs, eliminates dependency or required investment in external network management systems. Instant is a turnkey business-grade Wi-Fi solution that works right out of the box.

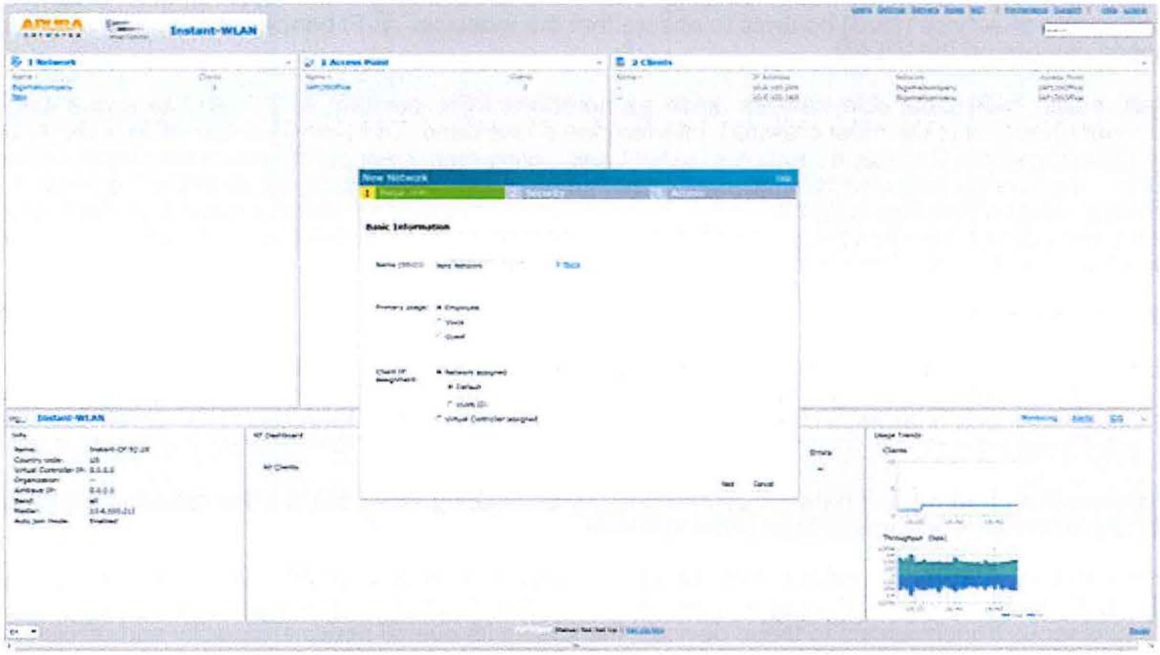
The Aruba Instant Virtual Controller technology provides security, consistently high performance, scalability, and other enterprise-class network access services without requiring a dedicated controller. Utilizing an adaptive, self-organizing wireless grouping, the Virtual Controller technology supports multiple Aruba Instant APs across wired LANs and over the air through the mesh, enabling the WLAN to scale effortlessly.

As with Mobility Controllers, Aruba Virtual Controller technology centralizes the functionality needed to configure and manage the Aruba Instant network. Aruba Virtual Controller technology delivers a wide range of enterprise-class WLAN capabilities required by enterprises that have multiple remote locations:

- Reliability – Aruba Instant is resilient to failure. If an Aruba Instant AP functioning as the primary Virtual Controller fails, another Aruba Instant AP automatically inherits the role of the primary Virtual Controller with no service disruption.
- Mobility – Users on Aruba Instant WLANs can roam campus-wide within the same Layer 2 domain in a Virtual Controller and across multiple Virtual Controllers. This is enabled by firewall and authentication-state synchronization across all Aruba Instant APs, as well as coordination of DHCP address allocation for NAT clients.
- Guest access – Aruba Instant provides automatic security classification for guests, eliminating the need to set up a guest VLAN. It automatically sets up a subnetwork to act as a DMZ that isolates the internal network from external networks and the Internet.
- Scalability – Offering self-organization and auto-configuration, adding Aruba Instant APs through a mesh or expanding to the outdoors is easy. At the same time, AirWave management lets IT centrally control thousands of Aruba Instant WLANs across multiple locations.
- Cloud-based firmware server – Aruba Instant receives firmware updates through the cloud server without the need for manual or laborious firmware updates. When a new image is available, the Aruba Instant user interface will indicate that an update is available.
- Built-in migration path – Aruba Instant offers a built-in migration path for organizations that want to transition to a centralized controller-based architecture. Aruba Instant APs easily convert to high-performance 802.11n/ac campus APs that are managed by a central Aruba Mobility Controller.

The Aruba Instant WLAN is comprised of multiple802.11n/ac APs with embedded Virtual Controller technology – which offer greater speed, coverage and reliability than legacy Wi-Fi. It is easily deployed as an overlay to an existing wired LAN in just a few minutes, eliminating the need for IT to redesign or modify the wired infrastructure.

Aruba Instant does not require IT expertise at distributed locations. All it takes to get an Aruba Instant WLAN up and running is to configure one Aruba Instant AP over the air using a simple wizard-driven process. Offering over-the-air provisioning, there's no need to modify an IP address to configure Aruba Instant. Just power up and connect an Aruba Instant AP to the LAN, and open a PC browser to automatically access the Aruba Instant user interface login page.



From this web-based interface, the user can assign SSIDs, and select authentication mechanisms. The entire set up takes less than five minutes. To configure additional Aruba Instant APs, simply connect and power them up. The first configured AP automatically becomes a primary Aruba Instant Virtual Controller and configures all the other APs. Aruba Instant is a fully distributed architecture. In the event of a primary Virtual Controller failure, another Aruba Instant AP automatically takes on the role with no disruption. The primary Virtual Controller operates like any other Aruba Instant AP with full WLAN functionality.

Adaptive Radio Management

Aruba's signature Adaptive Radio Management (ARM) technology automatically manages the WLAN's 2.4-GHz and 5-GHz radio bands to optimize Wi-Fi client performance and mitigate RF interference. It also ensures that each Aruba Instant AP uses the optimal channel- and transmit-power for its RF environment. ARM™ additionally offers priority traffic handling, channel load-balancing, band steering, airtime fairness and other quality-of-service (QoS) controls to ensure that the available Wi-Fi bandwidth is fairly distributed to all mobile devices on the WLAN.

Too often, newer 5-GHz-capable devices, such as notebook PCs, connect at 2.4 GHz to a dual-band network, even though it is the most crowded, interference-prone band. To rectify this, the ARM technology in Aruba Instant steers 5-GHz-capable clients to that band, giving them clear conditions, while clients limited to 2.4 GHz – such as bar code readers, Wi-Fi phones and older PCs – gain capacity as that band becomes less crowded. ARM also offers automatic application-detection capabilities, which enable it to distinguish voice and video from data traffic so that appropriate QoS mechanisms can be applied to ensure that latency-sensitive applications have sufficient network resources at all times.

ClientMatch Technology

Aruba's patented ClientMatchTM technology continuously gathers session performance metrics from the mobile devices such as location, device type, network congestion and interference. These metrics are then used to intelligently steer individual client to the best access point with the strongest Wi-Fi signal as users move.

ClientMatch optimizes client and network performance by eliminating sticky clients thus reducing helpdesk calls and doesn't require any specialized client software.

The Aruba 802.11ac Wave 2 Instant APs deliver enhanced multi-user MIMO (MU-MIMO) enhanced ClientMatch. By grouping MU-MIMO capable devices on the same stream, the network can take advantage of the simultaneous transmissions to these devices, increasing its overall network capacity and efficiency. These Wave 2 Instant APs also have an integrated BLE Beacon to remotely manage battery-powered Aruba Beacons for advanced location and wayfinding applications.

Security

Authentication and Encryption

Aruba Instant supports over-the-air authentication using pre-shared keys or 802.1X, which uses WPA2 for strong security and an internal or external RADIUS server.

Each Aruba Instant AP has an instance of a free RADIUS server that maintains a distributed database of up to 256 users. When using internal RADIUS for 802.1X authentication, customers can load certificates and terminate EAP-PEAP, EAP-TTLS and LEAP.

Organizations that use external RADIUS can use the Aruba Instant with a dynamic RADIUS proxy that leverages Virtual Controller technology to present the entire Aruba Instant network to the authentication back end. Aruba Instant RADIUS proxy ensures that the RADIUS client identity remains the same if a Virtual Controller fails, eliminating the need to modify the authentication back end.

Alternately, enterprise organizations with remote sites can configure each Aruba Instant AP as a RADIUS client so they can perform distributed RADIUS authentication without going through the Virtual Controller.

For authentication on a guest network, Aruba Instant provides a captive portal, which can authenticate guests against an internal database or an external authentication engine. In addition to authentication, Aruba Instant supports standard TKIP and AES as methods of encryption for wireless traffic.

Integrated Firewall

The Aruba Instant integrated firewall inspects traffic from each user session and allows or denies that traffic before it traverses the wired and wireless network. The firewall monitors all data entering or leaving the network, blocks data that does not satisfy specified security policies, and prevents unauthorized users from accessing the enterprise network.

Administrators use a simple firewall policy language to define access rules, which can be applied to an SSID or WLAN, such as the guest or employee network. Users are subject to access rules defined for the SSID to which they connect. The firewall also limits packets and controls bandwidth for different classes of users, such as students and guests.

Traffic Separation

Aruba Instant supports up to six SSIDs per Virtual Controller, which gives enterprise organizations the flexibility to separate WLAN traffic based on user role and traffic type. For example, school district employees can be assigned to one SSID, students to another, and guests to a third.

Similarly, voice and video traffic can be assigned to a specific SSID and given high-priority handling. Setting up multiple SSIDs is easy by following the wizard-driven steps in the Aruba Instant user interface.

To further simply configurations, Aruba Instant includes a special setting to create a voice SSID. This voice SSID automatically establishes the proper SIP application-layer gateways (ALGs) in the firewall policy and sets the highest QoS parameter.

In traditional wireless environments, an SSID is associated with a VLAN. However, Aruba Instant gives operators the option to associate an SSID with a user group, traffic type, or a VLAN. Specifying VLANs on the WLAN automatically enables the required trunking and tagging for the wired network.

Wireless Intrusion Protection

Aruba Instant includes a wireless intrusion protection system that safeguards the network from unauthorized or rogue APs and clients, and other devices that can potentially harm network operations.
The wireless intrusion protection capability also logs information about unauthorized APs and clients, and generates reports, making Aruba Instant fully PCI compliant. To prevent malicious APs from associating with network, administrators can turn on rogue AP prevention and disable the auto-join function, which ensures that only authorized Aruba Instant APs are allowed to connect.

Application Visibility and Control

The Aruba Instant AppRF™ technology intelligently monitors application usage and web traffic to secure and optimize network performance.

AppRF is Aruba's custom-built layer 7 firewall. It consists of integrated Deep Packet Inspection (DPI) functionality as well as a cloud-based Web Policy Enforcement (WPE) service. Each IAP has its own DPI engine which performs packet analysis and classification. They are also connected to Aruba's web-based URL database aruba.brightcloud.com for web category caching and verifying the reputation of URLs accessed by clients on the network. In conjunction with WPE, DPI provides the ability to analyze and identify applications, application categories, web categories, web reputation, and web URLs based on client data packets. Traffic shaping policies such as bandwidth control and per-application QoS can be defined for unique client roles. E.g. bandwidth-hungry applications may be blocked on a guest role within an enterprise. AppRF also enables compliance with privacy standards such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and Children's Internet Protection Act (CIPA). AppRF provides insight into over 2,500 apps, including apps like GoToMeeting, Box, Lync, SharePoint, and Salesforce.com.

Deep packet inspection (DPI) monitors mobile app usage and performance while optimizing bandwidth, priority and network paths in real time – even for apps that are encrypted or appear as web traffic. DPI is vital to understanding usage patterns that may require changes to network design and capacity.

AppRF typically will be used in a session acl which in turn will be used in a user-role. When user initiated traffic matches the signature of the App that is supported by our DPI engine, the session is blocked/permitted based on the action defined in the ACL.

The support of 'new' apps is tied to an update to the DPI engine itself, which requires IAP code update. The exact process of how 'new' apps are added to the DPI support is not something I can comment on, but the DPI engine is a 3rd party package that integrates within IAP code.

Content Filtering

Web content filtering is a function of Aruba's partnership with Brighcloud (webroot). URLs that IAP is unable to find reputation for within its local cache, it reaches out to bright cloud and fetches reputation in real time. Just like an App can be used in an ACL to perform deny/permit action on, webcc 'reputation' and 'category' can be chosen while building an ACL, URL that matches the 'reputation' and/or 'category' in the ALC is 'filtered' – meaning, either denied or allowed based on choice of action.

With content filtering, administrators can create Internet access policies that allow or deny user access to web sites based on categories and security ratings. Content filtering also prevents known malware hosts from accessing the WLAN, reduces bandwidth consumption and improves employee productivity by limiting access to certain web sites.

- Filter up to 55 web categories – including adult, proxy, peer-to-peer and social networking – and custom domain lists.
- Prevent access to servers that host and distribute malware.
- Block botnet command and control points to mitigate data leaks from infected devices.
- Create bypass codes that allow select users to access blocked sites.
- Report on blocking and overall usage with optional daily emails.
- Connect to the global OpenDNS cloud-based service with zero downtime or added latency.

For optimum performance, Aruba Instant APs store responses from the OpenDNS servers, and search cache memory when they receive an access request. If a suitable record is found, the Aruba Instant AP responds accordingly, accelerating the response by eliminating the need to contact the DNS server again.

Operating System Fingerprinting

The OS fingerprinting feature gathers information about each client connected to an Aruba Instant WLAN to determine what OS the client is running. This information enables IT to identify rogue clients, including clients running an OS not allowed on the company network, as well as clients with an outdated OS. OS fingerprinting also helps IT locate and patch clients with specific OS versions that have known vulnerabilities to fortify enterprise network security.

Instant Network Management & Monitoring

Aruba Instant provides a choice of network management tools:

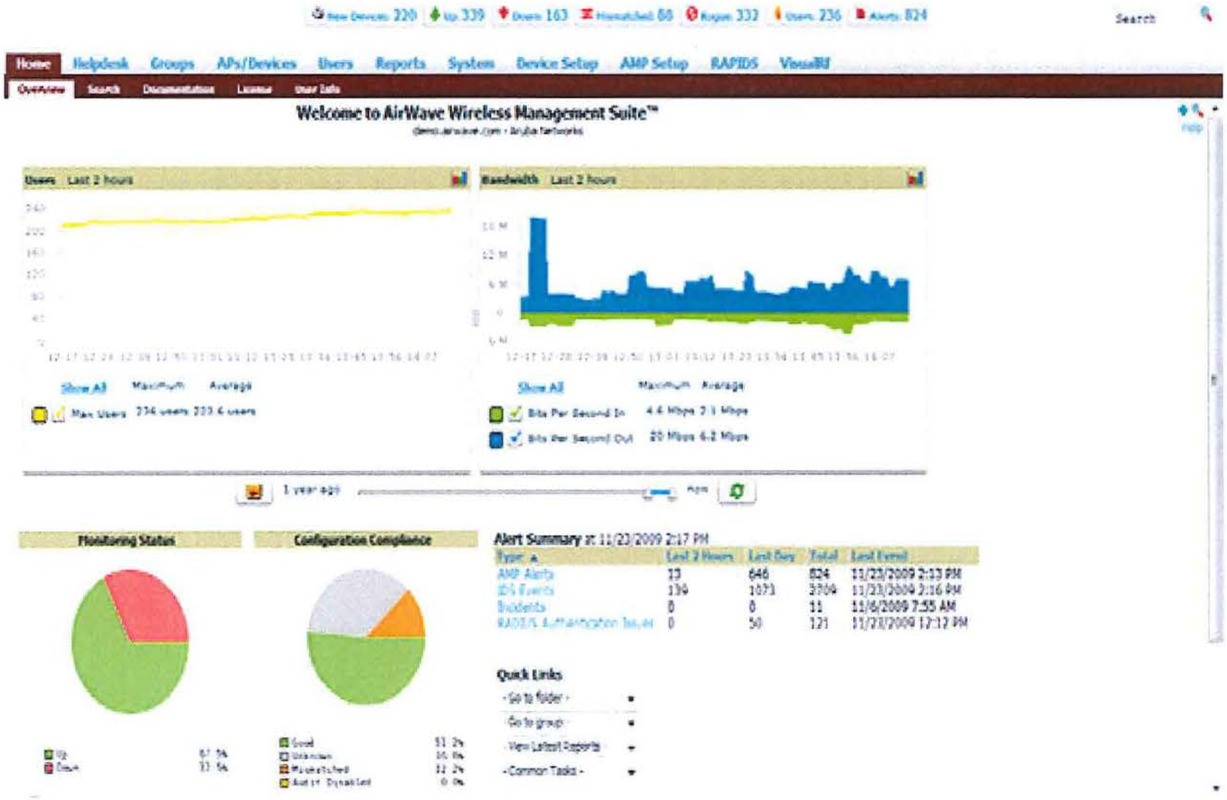
- Built-in UI provides a no-cost management solution that is ideal for managing a few Instant networks separately.
- Aruba Central offers a cloud management option that makes managing multiple networks and sites centrally.
- Airwave delivers rich wireless and wired network management for a multivendor infrastructure.

Network Management

Local area networks were designed to connect enterprise users sitting at their desks to servers located in a nearby data center. In today's dynamic, distributed enterprise, users have moved away from their desktops. They use multiple mobile devices to connect to the network on campus, in branch offices, at home and on the road. Their applications run not only on servers elsewhere in the building, but also data centers hundreds of miles away and in the cloud. To support these demanding mobile users, IT professionals are re-architecting their networks, using new wireless technologies like 802.11ac to deliver mobility while reducing the cost of the network infrastructure.

The consequences of downtime are significant. Downtime impacts worker productivity. And it increases the support burden for everyone in IT, from the network engineers responsible for managing the infrastructure to the service desk staff who answer the phone when users experience connectivity problems.

Too often, network operations departments are struggling to manage their mission-critical wireless networks with tools designed for the static wired networks of the 1990s or with proprietary wireless element management systems designed by hardware vendors. The fundamental problem is that today's mobile users break yesterday's port-based network management models. Traditional element management systems were never designed to answer the question critical to operating networks for mobile users: Who is connected? Where are they located? What devices are they using, with what drivers and operating system patches? Are they properly authenticated? What's happening in the RF environment? How much bandwidth is available and how much is being used?



Alert Summary at 11/23/2009 2:17 PM

Type ▲	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	33	646	824	11/23/2009 2:13 PM
IDS Events	134	1073	3704	11/23/2009 2:16 PM
Incidents	0	0	11	11/6/2009 7:55 AM
RADIUS Authentication Issues	0	50	121	11/23/2009 12:12 PM

Using outdated tools to manage wireless networks leads to predictable results: frequent escalations of routine issues to scarce network engineering resources, poor network performance and rapidly increasing support costs. With thousands of new wireless users and whole new categories of wireless devices coming online — VoIP phones, printers, handhelds, asset tags and more — the problem is getting worse every day.

To support a mission-critical wireless network and a mobile user population without adding substantial IT headcount, you need a new approach to network management — an approach supported by intelligent, user-centric management tools designed specifically to address the unique requirements of a mobile world. You must be able to delegate responsibility across the IT organization — letting the service desk troubleshoot routine issues so that network engineering staff can work on the most difficult and important problems.

Aruba has two separate offerings for our customers to manage their Aruba equipment. AirWave was first launched in 2003, and has grown to be a very full-featured, multi-vendor management solution. Aruba Central was launched in 2013, and is a separate cloud-based management tool for managing Aruba Instant APs and Aruba Switches.

The Cloud and Aruba Central

Aruba Central offers a simple, secure and cost-effective way to manage and monitor Aruba Instant APs and switches. It also has advanced capabilities like customizable guest Wi-Fi, Aruba Clarity and presence analytics for smarter decision making. With Aruba Central, you can get your wired and wireless networks up and running in minutes with intelligent Zero Touch Provisioning. The intuitive dashboards, along with reporting, maintenance, and firmware management makes it easier to manage networks of all sizes.

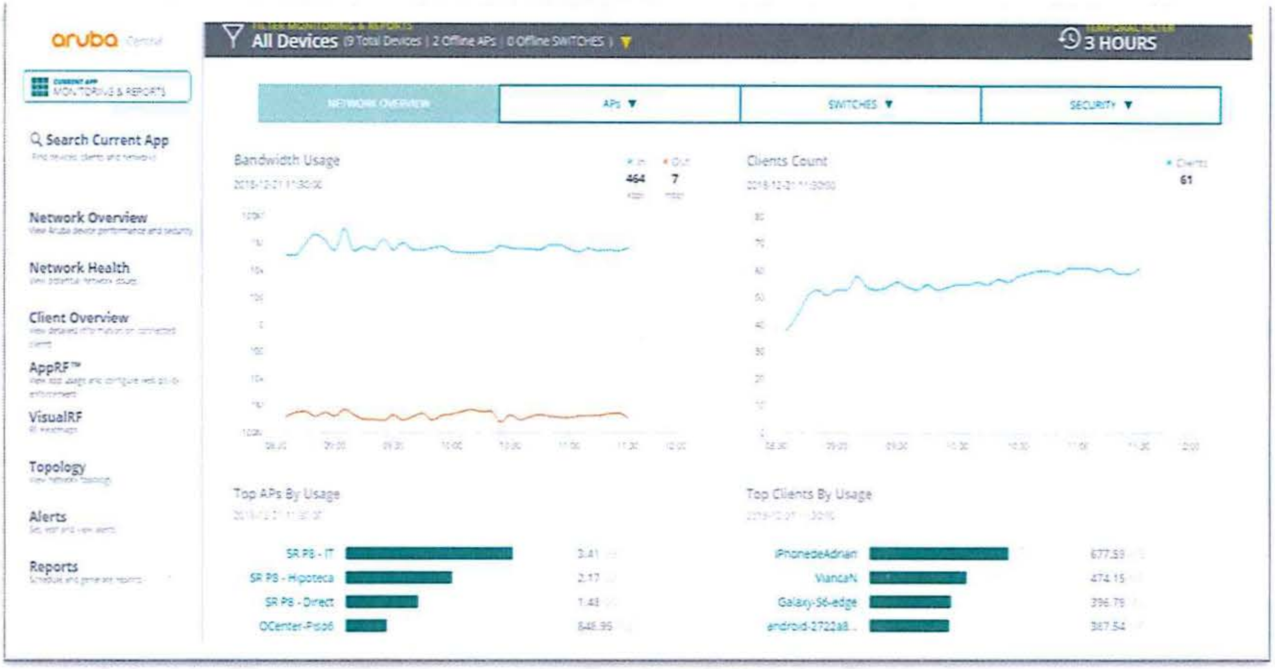
The Cloud and Aruba Activate

Aruba Activate is a Cloud Based Service designed to enable more efficient purchasing, deployment, and maintenance of their Aruba devices. The Aruba Activate service significantly reduces deployment time by automating device provisioning, firmware upgrades, and inventory management. With Aruba Activate, Instant APs are factory-shipped to any site and configure themselves when powered up.

Aruba Central Cloud Management

Aruba Central is a cloud-based platform that enables PRDE to manage the proposed Aruba Wi-Fi network. Designed as a software-as-a-service (SAAS) subscription the solution comply and exceed with all PRDE requirements.
Central provides a standard web-based interface that offers PRDE a simple, secure and cost-effective way to manage and monitor the Aruba Instant wireless LANs, as well as integrated capabilities such as customizable guest Wi-Fi and application analytics. Aruba Central offers PRDE a simple, secure and cost-effective way to deploy, manage and monitor wired and wireless networks. Key considerations for any organizations to consider are zero touch provisioning, centralized visibility and the ability to offload capital and operating expenses.

Aruba Central not only helps get the network up and running quickly, but the intuitive dashboards make monitoring, troubleshooting, and firmware management easy, from anywhere – no onsite technical expertise required. Advanced capabilities not typically included in network management solutions, like customizable guest access, user connectivity insights, and analytics that identify user presence and traffic, extend the value of the cloud-based solution.



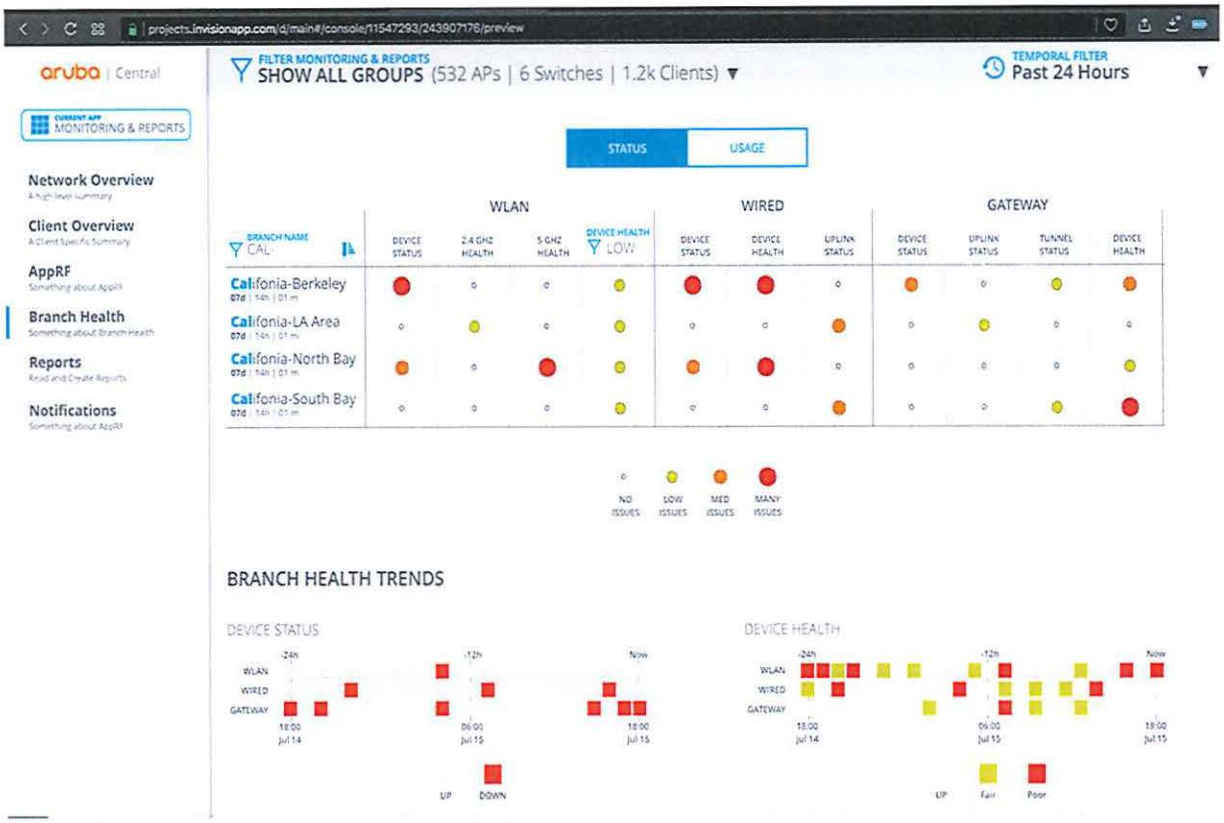
Simplified Network Management

Very often, cloud solutions are light-weight products stripped down to a bare minimum to satisfy a checklist. While simplicity is one of the important components of a cloud management service, there's a lot more you should demand from a business-grade solution.

Aruba's cloud-management solution delivers a perfect combination of task oriented interface tools, granular configuration capabilities, and enterprise-class network management visibility – along with the cost and operational benefits of a cloud service.

Aruba Central simplifies network management for Department of Education WiFi network by extending anywhere-anytime access to ensure network is performing efficiently.

- Zero-touch provisioning makes network setup fast and easy. Simply preconfigure Instant APs and switches in Central. Ship APs and switches directly to remote sites and when powered up, they get their configuration and firmware from Central.
- Single dashboard for monitor APs, switches and clients simplifies isolating problems and troubleshoot quickly.
- Wireless Intrusion Detection System (WIDS) to identify rogue devices on the network.
- Streamlined and automated maintenance and firmware management with one-click or scheduled updates.
- Network, application and security reports that can be easily scheduled and shared for low-effort monitoring. Includes Payment Card Industry (PCI) reporting for compliance to regulatory mandates
- Report Generation.
- Centralized configuration of APs and Aruba switches.
- Simplified device manage
- Monitoring
- Support with different languages (English, Spanish) minimum
- Reports as (specified in Section IV, Paragraph 3)
- Auto schedule and email


projects.invisionapp.com/d/main#/console/11547293/243907176/preview
aruba | Central
CURRENT APP MONITORING & REPORTS
Network Overview
A high level summary
Client Overview
A Client Specific Summary
AppRF
Something about AppRF
Branch Health
Something about Branch Health
Reports
Read and Create Reports
Notifications
Something about AppRF
FILTER MONITORING & REPORTS
SHOW ALL GROUPS (532 APs | 6 Switches | 1.2k Clients)
TEMPORAL FILTER
Past 24 Hours
STATUS
USAGE

	WLAN				WIRED			GATEWAY			
BRANCH NAME CAL	DEVICE STATUS	2.4 GHZ HEALTH	5 GHZ HEALTH	DEVICE HEALTH LOW	DEVICE STATUS	DEVICE HEALTH	UPLINK STATUS	DEVICE STATUS	UPLINK STATUS	TUNNEL STATUS	DEVICE HEALTH
Califonia-Berkeley 07d | 14h | 01 m	🔴	○	○	🟡	🔴	🔴	○	🟠	○	🟡	🟠
Califonia-LA Area 07d | 14h | 01 m	○	🟡	○	🟡	○	○	🟠	○	🟡	○	○
Califonia-North Bay 07d | 14h | 01 m	🟠	○	🔴	🟡	🟠	🔴	○	○	○	○	🟡
Califonia-South Bay 07d | 14h | 01 m	○	○	○	🟡	○	○	🟠	○	○	🟡	🔴

○ NO ISSUES 🟡 LOW ISSUES 🟠 MED ISSUES 🔴 MANY ISSUES

BRANCH HEALTH TRENDS

Aruba Central Mobile App

Aruba Central free mobile app extends Aruba Central cloud management to your iOS/android device, letting you easily Onboard and monitor devices.

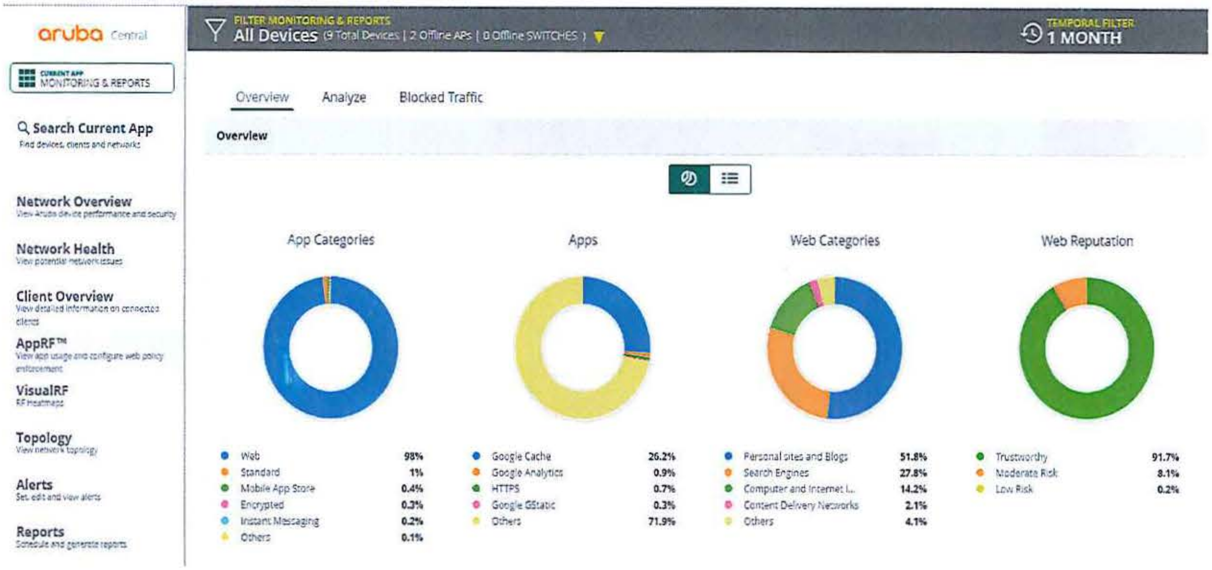
- Simplify device on-boarding by scanning the barcode of your device - IAP / Switch and add it to your network
- Monitor the details of Aruba Wireless Access points and its clients on your network
- Monitor Switches
- AppRF Graphs

Enterprise-Class Application Control

PRDE want to know how the WiFi network is used and control application and web traffic usage directly on the Access Point? Aruba AppRF is a built-in feature that helps optimize app use and unwanted web surfing – no need for additional solutions and appliances.

- View, analyze and control client traffic based on individual applications, as well as categories of application types, websites visited, and website reputation.
- Control priority, bandwidth and access rules to apps and websites based on configured roles.

AppRF on Central allows PRDE secure and optimize your network performance with application-level intelligence and web URL classification. The dedicated dashboard is designed to visualize and analyze application traffic to define and enforce granular access policies.


aruba Central
CURRENT APP
MONITORING & REPORTS
Search Current App
Find devices, clients and networks
Network Overview
View Aruba device performance and security
Network Health
View potential network issues
Client Overview
View detailed information on connected clients
AppRF™
View app usage and configure web policy enforcement
VisualRF
RF Heatmaps
Topology
View network topology
Alerts
Set, edit and view alerts
Reports
Schedule and generate reports
FILTER MONITORING & REPORTS
All Devices (9 Total Devices | 2 Offline APs | 0 Offline SWITCHES)
TEMPORAL FILTER
1 MONTH
Overview
Analyze
Blocked Traffic
Overview
App Categories
Apps
Web Categories
Web Reputation

App Categories	
● Web	98%
● Standard	1%
● Mobile App Store	0.4%
● Encrypted	0.3%
● Instant Messaging	0.2%
● Others	0.1%

Apps	
● Google Cache	26.2%
● Google Analytics	0.9%
● HTTPS	0.7%
● Google GStatic	0.3%
● Others	71.9%

Web Categories	
● Personal sites and Blogs	51.8%
● Search Engines	27.8%
● Computer and Internet I...	14.2%
● Content Delivery Networks	2.1%
● Others	4.1%

Web Reputation	
● Trustworthy	91.7%
● Moderate Risk	8.1%
● Low Risk	0.2%

Zero-Touch Provisioning

Aruba ZTP simplify network set up by directly shipping Aruba Instant APs to remote sites. Any non-technical person can simply unpack and power up the APs as they automatically download their configuration and firmware from Aruba Central and the network is up and running in minutes.

Aruba Installer Mobile App: If there are multiple sites to deploy, business may require more time and manual effort to coordinate and manage site installations. The Aruba Installation Management service simplifies and automates site deployments, and helps IT administrators manage site installations with ease.

The Aruba Installation Management service includes the following components:

> Install Manager on Central portal—Intended for IT administrators who oversee the installation management activities in an organization. Using Install Manager, network administrators can create installer profiles, assign site deployments to installers, and monitor deployment status for each site from a remote location. Central users can access the Install Manager application from the app selection pane in the UI.
>
> Aruba Installer mobile app—Intended for the installation personnel who deploy devices on a site. The Aruba Installer mobile app allows the installers to scan devices and add them to the provisioning network. The Aruba Installer mobile app is available for downloads on Apple® App Store and Google Play Store.

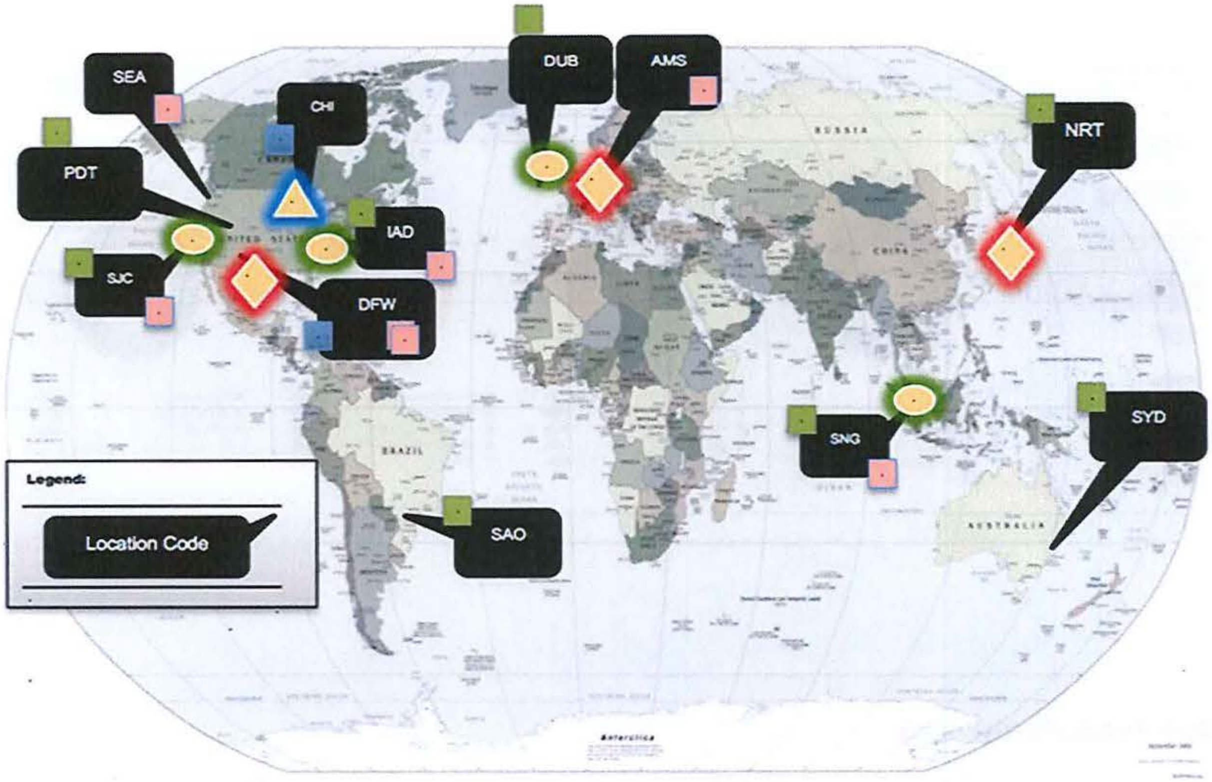
Security and High-availability

Aruba Central, designed from the ground up as a cloud application, ensures highest possible availability.

- Web-scale database design for responsive performance, even when working with huge amounts of data.
- Redundancy with clustering and distributed to multiple data centers by multiple providers. Aruba Central ensures uninterrupted service. If one provider experiences performance issues, others remain available and Aruba Central continues seamlessly.
- Global reach with data center locations around the world.
- HTTPS connection with strong mutual authentication using certificates to ensure secure communication with Aruba products. Certificates are stored in Trusted Platform Module (TPM)

Eom

chips on Aruba hardware for the highest level of protection.



Cost-effective Management

With Aruba Central, everything from setting up the network to monitoring and maintaining it is effortless. Whether managing one site or a thousand remote sites, one single console that can be accessed from anywhere gives you the visibility and control you need.

With Zero Touch Provisioning, Puerto Rico Department Education can directly ship Aruba Instant APs to remote sites where anyone with no technical expertise can simply unpack, power them up and connect to the network. Configuration is automatically pushed from Central – so the Communication network is up and running in minutes.

A simple dashboard provides an overview of your network, along with client and application performance monitoring views. Detailed drill-downs help isolate problems and identify rouge devices – ensuring top-notch performance with a few simple clicks.

Built-in reporting, including Payment Card Industry (PCI) reports for businesses that require regulatory compliance for secure transactions and continuous network monitoring is simple.
With flexible firmware management, configuration templates and admin user management, ongoing network administration is fast and efficient.

These points translate to lower upfront costs and a predictable subscription model.

- Elimination of truck roll costs with zero-touch-provisioning
- Subscription availability in 1/3/5/7/10-yr options include tech support for both management and APs.

Centralized Maintenance & Firmware Updates

Comply with maintain complete control of the network by choosing how to organize and when to automate maintenance functions.

- Create groups and tag devices with labels to simplify firmware management and configuration.
- Choose to schedule or perform on-demand firmware updates.
- Provide role-based access to different administrators with varied levels of privileges to view and manage.

A Smart Cloud Investment

Designed from the ground up for the cloud, Aruba Central's web-scalable database makes working with huge amounts of data easy.

Built-in redundancy with clustering and distribution across multiple data centers by multiple providers ensures you're always up and running. Without additional network management hardware and software to install, update and maintain, PRDE can take advantage of the OPEX model with cloud subscriptions available in 1yr/3yr/5yr options with options for base management as well as services subscriptions which includes full technical support including phone support for any technical issues for Central and for managing APs and switches.

Aruba Central is available in two operational modes:

- Standard Enterprise Mode — The Standard Enterprise Mode provides a complete view of the devices that are monitored and managed by Central. It also allows end-end provisioning, management, monitoring, and maintenance operations for the devices associated with the Central customer accounts.
- Managed Service Mode — The Managed Service Portal provides a consolidated view of the networks of customers for the Managed Service Provider. The service provider administrators can manage devices, and subscriptions associated with the customer accounts within their network.

For additional reference information please refer to Appendix A.

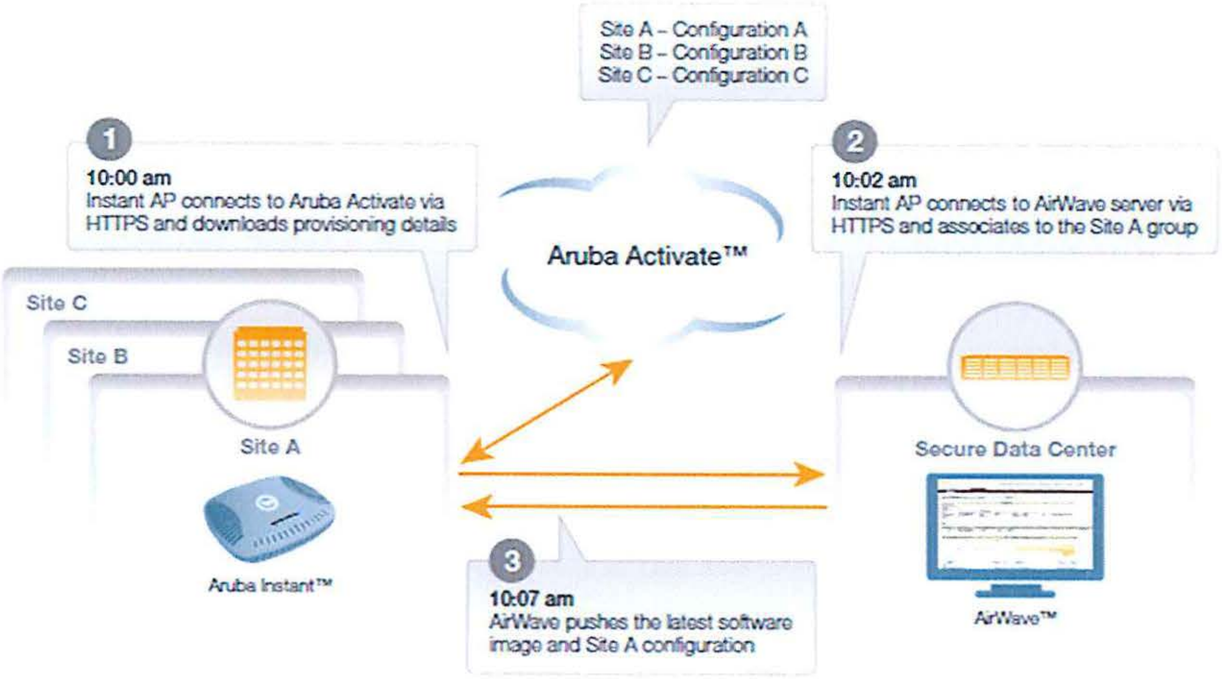
Eom

Aruba Activate Cloud Service

A free cloud based service designed to enable more efficient purchasing, deployment, and maintenance of Aruba devices. Aruba Activate provisions APs and switches with zero touch and automates firmware upgrades and inventory management. This enables Aruba WLANs to be deployed at unprecedented speed and without onsite IT support at any number of locations worldwide. The entire process takes only a few minutes and the results are impressive. Aruba Activate slashes the deployment time of Aruba Instant APs and the newest generation of Remote APs (RAPs) by 65%. It also reduces the total cost of enterprise WLAN ownership by up to 42%.

The proposed Aruba APs to the PRDE will be automatically added to the customer's inventory in Aruba Activate and associate with proper provisioning rules. The APs are then factory-shipped to their destination, where a non-technical person takes one AP out of the box and connects it to the Internet. That AP retrieves its provisioning data from Aruba Activate and then uses that information to obtain its configuration from Aruba Central any AirWave™ server or Aruba Mobility Controller. The AP then pushes that configuration out to all other APs in the WLAN. The Aruba Activate AP provisioning workflow follows a simple three-step process:

- **Step 1: Create locations and define provisioning rules** - Log into Aruba Activate to find the list of APs your organization has purchased. To assign APs to a specific configuration master – an AirWave server or Mobility Controller – folders must be defined in Aruba Activate so you can group APs based on their geographic locations. Rules let you define how APs can contact their configuration master to retrieve firmware and configuration settings. You can also use rules to automatically assign APs to specific locations.
- **Step 2: Select devices** - Aruba Activate allows you to sort and filter all APs in your device list, making it easy to display the APs you want to assign to any defined folder.
- **Step 3: Assign devices to folders** - Activate makes it easy to assign one or multiple APs to a folder by highlighting the APs and using the move-to-folder function. When APs are moved into a folder, they immediately inherit all the parameters defined for that folder.


Site A – Configuration A
Site B – Configuration B
Site C – Configuration C
1
10:00 am
Instant AP connects to Aruba Activate via HTTPS and downloads provisioning details
Aruba Activate™
2
10:02 am
Instant AP connects to AirWave server via HTTPS and associates to the Site A group
Site C
Site B
Site A
Aruba Instant™
Secure Data Center
AirWave™
3
10:07 am
AirWave pushes the latest software image and Site A configuration

SERVICE PROPOSAL: Statement of Work Information

Solution Overview

This project is intended to provide Services as they relate to Customer's PRDE-OSIATD-2018-003-Wireless Equipment and services.

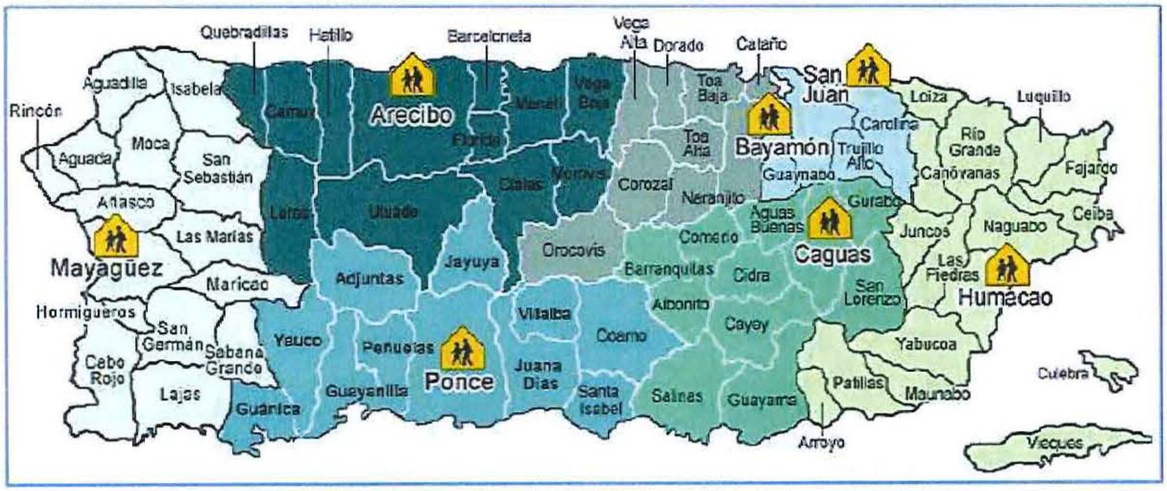
The Puerto Rico Department of Education (the "Department," or "PRDE") is the government agency that directly runs and operates Puerto Rico's public school system. Information concerning the approximate size of the PRDE school system is as follows:

THE PRDE SCHOOL SYSTEM*	
Students:	300,000
Schools:	857
Educators:	25,000
Educational Regions:	7

*Estimates

The Department intends to purchase and install up to 70,000 indoor (56,000) and outdoor (14,000) wireless access points during the 2018-2019 school year. The equipment is expected to provide full wireless coverage in all of the Department's 857 schools and 37 non-instructional facilities (including the 7 Region Offices), and to support approximately 160,000 tablets and laptops being purchased for Department schools. Also, the Department intends to purchase and install 857 devices for Network Access Control, to provide more granular security to the school's users. Also, the bandwidth in each school is being upgraded up to 750 MB during the 2018-2019 school year, and potentially up to 1 GB the following year to support increased network usage.

PRDE has 7 Regions and 28 Districts.



This project includes the implementation of the following products and services:

- Hardware equipment from Aruba.
- Design and Implementation.
- Services and Support

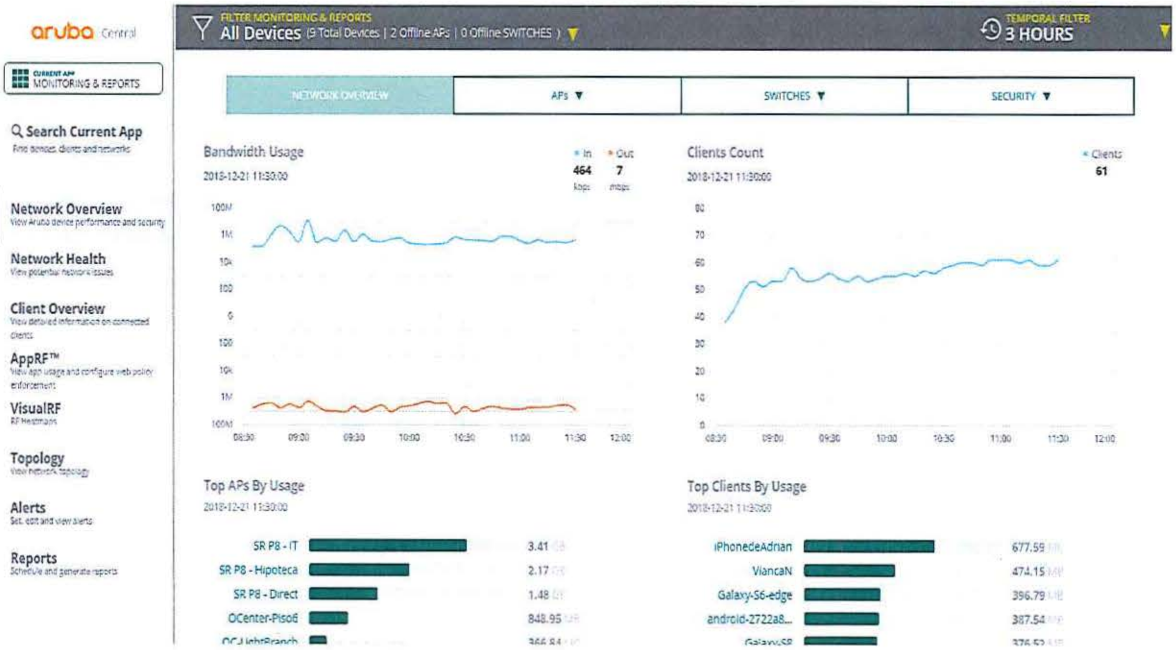
CLARO PR will create a project plan and project schedule and determine the appropriate mix of technical and business resources necessary to implement the project.

Aruba Central Cloud Management

Aruba Central is a cloud-based platform that enables PRDoE to manage the proposed Aruba Wi-Fi network. Designed as a software-as-a-service (SAAS) subscription the solution comply and exceed with all PRDoE requirements.

Central provides a standard web-based interface that offers PRDoE a simple, secure and cost-effective way to manage and monitor the Aruba Instant wireless LANs, as well as integrated capabilities such as customizable guest Wi-Fi and application analytics. Aruba Central offers PRDoE a simple, secure and cost-effective way to deploy, manage and monitor wired and wireless networks. Key considerations for any organizations to consider are zero touch provisioning, centralized visibility and the ability to offload capital and operating expenses.

Aruba Central not only helps get the network up and running quickly, but the intuitive dashboards make monitoring, troubleshooting, and firmware management easy, from anywhere – no onsite technical expertise required. Advanced capabilities, not typically included in network management solutions, like customizable guest access, user connectivity insights, and analytics that identify user presence and traffic, extend the value of the cloud-based solution.



Aruba Hardware and Software Proposed

Aruba will provide the following components:

Part Number	Description	Quantity
JX967A	Aruba AP-375 (US) Outdoor AP	14000
JW054A	AP-270-MNT-H1 AP-270 Series Outdoor AP Hanging or Tilt Install Mount Kit	14000
JY926AAE	Aruba Central Device Management 1 Token 3 Year Subscription E-STU	70000
JY929AAE	Aruba Central Cloud Services 1 Token 3 Year Subscription E-STU	70000
JX946A	Aruba IAP-305 (US) 802.11n/ac Dual 2x2:2/3x3:3 MU-MIMO Radio Integrated Antenna Instant AP	56000
JW047A	AP-220-MNT-W1W Flat Surface Wall/Ceiling White AP Basic Flat Surface Mount Kit	56000
JZ399AAE	Aruba ClearPass Cx000V VM Appliance E-LTU	4
JZ405AAE	Aruba ClearPass NL AC 10K CE E-LTU	20
JZ441AAE	Aruba ClearPass NL OB 10K USR E-LTU	15
JZ477AAE	Aruba ClearPass NL OG 10K EP E-LTU	5
JW470AAE	Aruba ClearPass Guest Custom Skin E-LTU	1

Table # 1

Requested Equipment and Services

Project Specific Deliverables

CLARO PR will provide the following Deliverables in the course of performing the Services described in this SOW.

- Kickoff
- Information gathering.
- Solution Plan and Design.
- Aruba Central Implementation provided by CLARO PR in table # 1
- Clearpass Implementation provided by CLARO PR in table # 1
- Solution testing & tuning in five (5) schools.
- Installation and Configuration of 70.000 APs provided by CLARO PR in table # 1
- Support Services by 3 years
- Account Management during the project
- Project Management

Kickoff

Deliverables

- Minutes of the project Kickoff meeting
- Milestones Plan: Project plan acceptance and completion of Kickoff meeting
- Format for information gathering and/or any other document that CLARO PR deems necessary for the implementation phase.

Acceptance Criteria

The team of CLARO PR will define formats and the protocol to be used which best suited to both parties.

Compliance of deliverables listed above.

- Kickoff meeting completed.
- Milestone Plan accepted.
- All deliverables that are documents or reports, shall be considered as accepted when presented as described in the documentation review process of this document.
- Acceptance must include the signature of customer's Project Manager in charge of this project.

Assumption

- The customer will give us Report of the Site Survey (SSV), based on the SSV will be determined equipment location, the report will contain physical and logical diagrams for the installation of the equipment and its components.
- The services will be provided at the schools defined in appendix during regular working hours. (Monday through Friday, from 8am to 5pm), excluding Holidays, on the Metropolitan area.
- The Customer's "liaison" will be responsible for scheduling any required customer personnel for meetings and/or interviews.
- All relevant Customer documentation will be made available to the project team when requested.
- The Customer will be responsible for relocating any of the equipment to be serviced, should this be required. Otherwise, CLARO PR cannot be responsible for any loss or damage of equipment during the relocation.
- The Customer will be responsible for delivering the schools with all the network (copper, fiber, POE-Switches, Cabinets, points of AP installations, etc.) in place and operating in optimal conditions prior to the installation of the AP´s
- No school will be installed if the network infrastructure is not complete.
- The Customer must guarantee access to the school for their installation.
- In case a revisit to the school is necessary because a faulty (NON-AP) network infrastructure the revisit will be invoiced.
- The Customer will be responsible for delivering the schools at least 40 schools per week.
- If for any reason the customer cannot deliver the requested 40 schools per week, the tentative project, delivered with the present proposal will be delayed at no penalty to CLARO PR.
- No request can be made to CLARO PR at the end to increase the installation throughput teams to cope for a shortage in school's availability.
- Once a school is finished, all the AP´s installed and functioning correctly, a report document for the school will be generated with the test protocol defined in the kickoff section of the project. Once that document is generated PRTC/Claro will have 10 working days to review the document and approved. If no answer is received the school installation and it correspondent service will be invoiced.
- If the schools have all the requested AP´s installed, working properly and the test protocol worked OK the school is considered finished and no last time requests will be accepted.
- Electrical and environmental conditions are appropriate for project implementation.
- Customer's Project Manager is responsible for the overall progress.
- Once the Site is accepted, the end customer is responsible for monitoring, management and diagnostic on a day to day basis.
- It's not included the Interaction and the configuration of third parties' products not covered by the initial "scope".
- It's not included any change to original design of the solution.
- In addition, we assume that all tasks to be done by third parties contracted by Customer will be coordinated by Customer, unless requested to CLARO PR, in which case will be billed on a time and material basis.

Information gathering

The initial information gathering is essential for the development of the design of the solution which will be implemented. The main objective is to obtain the necessary technical information relate to current network infrastructure and service objectives.

This activity includes the following tasks:

a. Meetings with the staff responsible for the project.

b. Definition of the conditions (physical, logical, and environmental) required to implement the solution.

c. Collect configuration information for each component, VLANs, associated ports, IP addressing, routing, security policies or any other information that is required for the configuration of the platform.

d. Obtaining of existing documentation related to the design of the solution.

e. Definition of the protocols currently used in the network and the necessary considerations for the equipment interconnection.

f. A Site Survey will be executed where required.

Deliverables

- Minutes of the project.
- Milestones Plan acceptance.
- Reports with the content collected.
- Format for information gathering and/or any other document that CLARO PR deems necessary for the implementation phase.

Acceptance Criteria

The team of CLARO PR will define formats and the protocol to be used which best suited to both parties.

Compliance of deliverables listed above.

- Minutes of the project accepted.
- Milestone Plan accepted.
- Reports with the content collected completed.
- All deliverables that are documents or reports, shall be considered as accepted when presented as described in the documentation review process of this document.
- Acceptance must include the signature of customer's Project Manager in charge of this project.

Assumption

- The customer will give us Report of the Site Survey (SSV), based on the SSV will be determined equipment location, the report will contain physical and logical diagrams for the installation of the equipment and its components.
- The services will be provided at the schools defined in appendix during regular working hours. (Monday through Friday, from 8am to 5pm), excluding Holidays, on the Metropolitan area.
- The Customer's "liaison" will be responsible for scheduling any required customer personnel for meetings and/or interviews.
- All relevant Customer documentation will be made available to the project team when requested.
- The Customer will be responsible for relocating any of the equipment to be serviced, should this be required. Otherwise, CLARO PR cannot be responsible for any loss or damage of equipment during the relocation.
- The Customer will be responsible for delivering the schools with all the network (copper, fiber, POE-Switches, Cabinets, points of AP installations, etc.) in place and operating in optimal conditions prior to the installation of the AP´s
- No school will be installed if the network infrastructure is not complete.
- The Customer must guarantee access to the school for their installation.
- In case a revisit to the school is necessary because a faulty (NON-AP) network infrastructure the revisit will be invoiced.
- The Customer will be responsible for delivering the schools at least 40 schools per week.
- If for any reason the customer cannot deliver the requested 40 schools per week, the tentative project, delivered with the present proposal will be delayed at no penalty to CLARO PR.
- No request can be made to CLARO PR at the end to increase the installation throughput teams to cope for a shortage in school's availability.
- Once a school is finished, all the AP´s installed and functioning correctly, a report document for the school will be generated with the test protocol defined in the kickoff section of the project. Once that document is generated PRTC/Claro will have 10 working days to review the document and approved. If no answer is received the school installation and it correspondent service will be invoiced.
- If the schools have all the requested AP´s installed, working properly and the test protocol worked OK the school is considered finished and no last time requests will be accepted.
- Electrical and environmental conditions are appropriate for project implementation.
- Customer's Project Manager is responsible for the overall progress.
- Once the Site is accepted, the end customer is responsible for monitoring, management and diagnostic on a day to day basis.
- It's not included the Interaction and the configuration of third parties' products not covered by the initial "scope".
- It's not included any change to original design of the solution.
- In addition, we assume that all tasks to be done by third parties contracted by Customer will be coordinated by Customer, unless requested to CLARO PR, in which case will be billed on a time and material basis.

Solution Plan and Design

Deliverables

- Kickoff meeting
- Milestone Plan
- Document Templates
- High Level Design document (HLD)
- Low Level Design document (LLD)

High Level Design

Creation of the preliminary high level diagrams of the work to be executed. The design will serve as an overall guidance to the architecture of the project. The design document will include general architecture diagrams with pointers for later detailed specifications. Detail configurations for each Site will be created later and is not included in this high level design. The document is commanded to give a fairly complete description, while maintaining a high-level view of the solution. Among other things, information contained in this document will be:

- Basic conceptual diagrams – Diagrams presenting the logical topology of network implementation.
- IP and VLAN scheme – VLANs and IP Networks used on different locations
- Routing strategy – The routing protocols and strategy to be implemented.

Low Level Design

Low-level design (LLD) is a component-level design process that follows a step-by-step refinement process. Low-level design is created based on the high-level design.

The data organization may be defined during requirement analysis and then refined during data design work. Post-build, each component is specified in detail.

During the detailed phase the logical and functional design is done and the design of application structure is developed during the high-level design phase.

Standard Operating Procedures (SOP)

Due to the nature of this project, which includes many repetitive procedures by separate teams, a series of Standard Operating Procedures are going to be put in place. The development and use of SOPs minimizes variation and promotes quality through consistent implementation of procedures. Some of the SOP's for this project are:

- Inventory management,
- SITE visit readiness evaluation,
- SITE equipment configuration,

- SITE equipment packaging and identification,
- SITE equipment handling and distribution.
- SITE Installation and validation instructions for implementer

Acceptance Criteria

The team of CLARO PR will define formats and the protocol to be used which best suited to both parties.

Compliance of deliverables listed above.

- Kickoff meeting completed.
- Milestone Plan accepted.
- Document Templates Accepted.
- High Level Design completed.
- Low Level Design completed.
- All deliverables that are documents or reports, shall be considered as accepted when presented as described in the documentation review process of this document.
- Acceptance must include the signature of customer's Project Manager in charge of this project.

Assumption

- The services will be provided at the schools defined in appendix during regular working hours. (Monday through Friday, from 8am to 5pm), excluding Holidays, on the Metropolitan area.
- The Customer's "liaison" will be responsible for scheduling any required customer personnel for meetings and/or interviews.
- All relevant Customer documentation will be made available to the project team when requested.
- The Customer will be responsible for relocating any of the equipment to be serviced, should this be required. Otherwise, CLARO PR cannot be responsible for any loss or damage of equipment during the relocation.
- The Customer will be responsible for delivering the schools with all the network (copper, fiber, POE-Switches, Cabinets, points of AP installations, etc.) in place and operating in optimal conditions prior to the installation of the AP´s
- No school will be installed if the network infrastructure is not complete.
- The Customer must guarantee access to the school for their installation.
- In case a revisit to the school is necessary because a faulty (NON-AP) network infrastructure the revisit will be invoiced.
- The Customer will be responsible for delivering the schools at least 40 schools per week.
- If for any reason the customer cannot deliver the requested 40 schools per week, the tentative project, delivered with the present proposal will be delayed at no penalty to CLARO PR.
- No request can be made to CLARO PR at the end to increase the installation throughput teams to cope for a shortage in school's availability.

- Once a school is finished, all the AP´s installed and functioning correctly, a report document for the school will be generated with the test protocol defined in the kickoff section of the project. Once that document is generated PRTC/Claro will have 10 working days to review the document and approved. If no answer is received the school installation and it correspondent service will be invoiced.
- If the schools have all the requested AP´s installed, working properly and the test protocol worked OK the school is considered finished and no last time requests will be accepted.
- Electrical and environmental conditions are appropriate for project implementation.
- This proposal does not include connections to the electrical systems.
- Customer's Project Manager is responsible for the overall progress.
- Once the Site is accepted, the end customer is responsible for monitoring, management and diagnostic on a day to day basis.
- It's not included the Interaction and the configuration of third parties products not covered by the initial "scope".
- It's not included any change to original design of the solution.
- In addition, we assume that all tasks to be done by third parties contracted by Customer will be coordinated by Customer, unless requested to CLARO PR, in which case will be billed on a time and material basis.

Aruba Central Implementation

Information Gathering

After the initial Kick-off, CLARO PR will start with the information gathering process. This process requires full information to the networks devices. The information obtained will help us to characterize the existing Wi-Fi network and stablish a more accurate topological diagram for DoE PR School's Network and Offices.

Topology Design

Taking this into consideration we are going to create a high-level conceptual diagrams that can be discussed on the initial kick-off and later-on edited during the design stage of this project.

Configuration of the Aruba Central

The CLARO PR Engineer will configure as the topology design is established the architecture of the platform of Aruba Central and the distribution of the schools.

Deliverables

- Aruba Central Implementation provided by CLARO PR in table # 1.
- Aruba Central Account definition and creation
- Configuration of the architecture of the platform (example)
  - District
    - Town
      - School
        - AP's
- Provisioning of the AP's in the platform
- Clearpass Integration
- Creation of the SSID
- Configuration of basic reports
- Tests and validation of the service
- Knowledge transfer

Aruba Central Sign in

For the Aruba Central Account definition and creation, we need to go to the Aruba Central website and enter the email account that are going to administer the platform. If is the first time of the account to login, the registration page is displayed. The CLARO PR Engineer will complete the registration process with the customer using the account information for administration. After the registration process is complete, a verification email with a link "Activate your Account" will be sent to the customer email account registered on the Aruba Central. If the email verification is successful, the Log in to Aruba central button is displayed. The platform is ready to be use.

Aruba Central Account configuration

To create a user and define the account the CLARO PR Engineer will click the Maintenance > User Management on the Aruba Central platform. On the User Management pane click to add the user. The Create User windows is displayed. The CLARO PR Engineer will enter the email address of the user given by the PRDE in the username text box. After the username we must select the group to which is going to be assign the user. Then we must select the user level to be assign to the new account. Admin as suggestion. We're able to create up to 3 account for the Aruba Central Platform for PRDE. The new user will receive a welcome email and proceed to the first deliverable **Aruba Central Sign in.**

Configuration the architecture of the platform

Aruba Central allows some configuration settings to be managed efficiently at the group level. For that reason, we will suggest creating a group level of District and adding the AP to that district. Using a nomenclature to the names of the AP we can add the configuration for each AP to be assigned to that district. And using labels we can display as this example of District > Town > School > AP's. The idea of using the Labels is to filter the AP's for monitoring and reporting purpose. We can use the label tags to identify the location of the AP's. The CLARO PR engineer will create the labels on the Label Management page on Global Settings of the Aruba Central. To add a new label, click on the + icon and the Create New label pop-ups opens. Create a site and then enter the name for the label. For each Site or school are going to be labels assign with their respective school names to their respective AP's.

For the groups on Global settings > device & subscriptions we can create the groups (districts) clicking on the icon next to all groups. The CLARO PR engineer will create new groups as districts where the AP's are going to be assign. That Groups will be a template for other districts in terms of configuration. The group will contains the configuration of the Network which include SSID's, IP addresses, DNS, DHCP, gateways, and other services to give internet access to the users.

Provisioning of the AP's in the Aruba Central platform

To provision the AP's the CLARO PR Engineer will assign any of the following types of subscriptions either through the Managed service portal or the Central Standard interface.

- Device Subscriptions- Subscription for the device to avail basic services such as device configuration, monitoring, reporting and analyzing application usage.
- Service Subscriptions- Subscription based services for apps such as Presence Analytics, Guest Access, and so on.

To assig the subscription acquires from PRDE the CLARO PR engineer will click Global Settings > Device & Subscriptions > Subscription Assignment. The Subscription Assignment page allow assign subscription for the devices or services for which PRDE have be subscribed

To assign the subscription to the device the CLARO PR engineer will move the slider to devices, select the device or devices to which you want to assign the subscriptions and click assign. To assign services the CLARO PR engineer will move the slider to network services and select the device or devices to which you want to assign the service subscription token. After selecting the desired services click assign and the AP is ready to be used and deployed to the school on the group that the AP belongs depending of the configuration for that group in Aruba Central Platform.

Clearpass Integration

The CLARO PR engineer will integrate the AP's clusters on each district in their respective groups as a NAD device on the Clearpass server to be able to authenticate students, teachers and guest on each school. To integrate the AP's Clusters the CLARO PR engineer must assign the AP's cluster as a NAD device on the network devices option of the Clearpass to work as an intermediary between the users and the Clearpass.

Configuration of basic reports

The CLARO PR engineer will create up to 3 reports in the implementation phase including Network summary reports, client inventory and Client Usage. To create those reports, the CLARO PR engineer will select report > configure reports and create a new report page is displayed. After entering the basic parameter like title, the engineer will select the type of report to be generated with the parameter necessary for, like example generate the network summary report. Each report can be generated on any interval of time. We can choose as the needs of PRDE the reports on an interval of One-time, Daily Interval, weekly interval, monthly interval, or yearly interval from repeat option. The reports are going to be generated for all device groups (districts) and send by email to the recipients that the PRDE choose to be delivered.

Tests and validation of the service

The test and validation will be performed after each configuration has been implemented. The CLARO PR team will create a plan for the implementation phase that includes 5 schools in which tests may be conducted with student, teachers and Guest accounts. It will consist of a pilot for that specific school that recreates the connection of a student, a teacher and a guest to that school. This will help us solve any problem before carrying out a massive deployment in the other districts and avoid delays in implementation.

Acceptance Criteria

The team of CLARO PR will define formats and the protocol to be used which best suited to both parties.

Compliance of deliverables listed above.

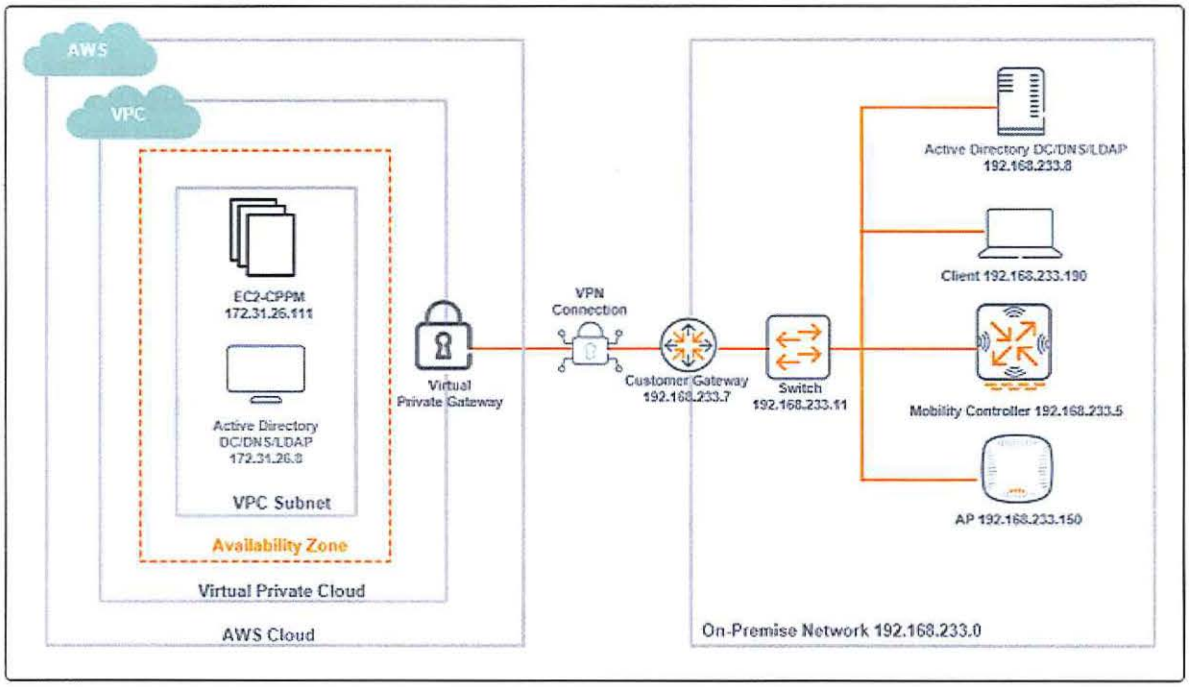
- Aruba Central Implementation completed.
- Aruba Central Account definition and creation completed.
- Configuration of the architecture of the platform completed.
- Provisioning of the AP's in the platform completed.
- Clearpass Integration completed.
- Creation of the SSID completed.
- Configuration of basic reports completed.
- Tests and validation of the service executed and documented.
- Knowledge transfer completed.
- All deliverables that are documents or reports, shall be considered as accepted when presented as described in the documentation review process of this document.
- Acceptance must include the signature of customer's Project Manager in charge of this project.

Aruba Clearpass on the Cloud Implementation

Clearpass Policy Manager is hosted on an AWS Virtual Private Cloud instance. Communication between controller and the Clearpass Policy Manager takes place through a secure VPN connection (IPsec tunnel) that is initiated by the controller. The figure below shows the test network setup that we used to test the Clearpass Policy Manager services on AWS.

In the example below, the network access device (NAD), which in this case is the Aruba controller, sits in a private network in the datacenter along with other APs, clients, DNS and a switch. The private gateway IP of this network is 192.168.233.7. On the other side is a VPC of subnet 172.31.0.0/16. This topology establishes a secure IPsec connection between the two networks to enable communication between the Aruba controller controller and the Clearpass Policy Manager on AWS. Clearpass is communicating with all authentication sources, NADs and clients over a VPN connection (IPSec), and the VPN tunnel is terminated on Virtual Private Gateway in the AWS Virtual Private Cloud (VPC) and on an on-premise Aruba wireless mobility controller (WLC).

Example Topology for ClearPass Policy Manager on AWS



Topology Design

Taking this into consideration we are going to create a high-level conceptual diagrams that can be discussed on the initial kick-off and later-on edited during the design stage of this project.

Deliverables

- Installation and configuration of Servers (4 Appliances)
- Implementation of 4 instance of EC2 to install 4 Aruba Clearpass.
- Aruba Clearpass Implementation provided by CLARO PR in table # 1.
- Configuration of the Clearpass Servers and administration services
- Creation of cluster combining 4 servers as 1 publisher and 3 subscribers
- Integration of Clearpass with Aruba Central
- Configuration of the Guest Captive Portal
- Integration with Active Directory
- Installation of the Digital Certificates
- Wireless 802.1X service policy (3)
- NAD integration
- On Board Configuration for BYOD with basic configuration
- Insight Configuration
- Tests and validation of the service
- Knowledge transfer

Configuration of the Aruba Clearpass

The CLARO PR Engineer will configure as the topology design is established, the architecture of the platform of Aruba Clearpass on the cloud.

The example topology for deploying Clearpass Policy Manager on AWS has the following requirements:

- ➢ A customer gateway: a configuration object in the virtual private cloud (VPC) that defines the on-premises VPN termination point.
- ➢ A virtual private gateway: a virtual router object that acts as the VPN termination point in the VPC.
- ➢ A VPN connection: a configuration object in the VPC that defines the VPN settings to be used when communicating with the Customer Gateway.
- ➢ A Site-to-Site IPSec map: a configuration object in the Aruba Mobility Controller that defines the customer gateway in the VPC as well as the VPN settings to be used when communicating with the VPC.
- ➢ Define your interfaces with two different subnets in the same availability zone in your VPC. Clearpass Policy Manager requires its eth0 and eth1 interfaces to be connected to different subnets.

Before you launch an instance of Clearpass Policy Manager using Amazon Web Services (AWS), you must perform the following tasks using the AWS management console.

Eow

1. Create a Customer Gateway on AWS
2. Add a Virtual Private Gateway to a VPC
3. Create a VPN Connection on AWS
4. Configure the Site-To-Site VPN Connection on the Gateway

Launch Clearpass Policy Manager on AWS from an AMI

The following section describes the procedure to launch an instance of Clearpass Policy Manager from an Amazon Machine Image (AMI) using the Amazon Web Services (AWS) console. These steps must be performed in the order shown in this document.

1. Obtain the Clearpass AMI
2. Locate and Identify your AMI
3. Launch an Clearpass Policy Manager EC2 instance
4. Choose an Instance Type
5. Configure Instance Details
6. Add Storage
7. Add Tags
8. Configure a Security Group
9. Review Instance Launch

Post-Launch Configuration Tasks in AWS

The following section describes the tasks that can be performed after you launch your Clearpass Policy Manager instance.

The procedure to create and attach a network interface or create and attach an EBS storage volume can be performed either as part of the launch setup, or after the Clearpass instance has already been launched.

1. Create and Attach an Elastic IP
2. Create and Attach an Elastic Block Store (EBS) Volume
3. Create a Security Group
4. Define and Configure Network Interfaces.

Acceptance Criteria

The team of CLARO PR will define formats and the protocol to be used which best suited to both parties.

Compliance of deliverables listed above.

- Servers installed and configured accepted.
- Aruba Clearpass Implementation completed.
- Configuration of the Clearpass Servers and administration services completed.
- Creation of cluster combining 4 servers as 1 publisher and 3 subscribers completed.

- Integration of Clearpass with Aruba Central completed.
- Configuration of the Guest Captive Portal completed.
- Integration with Active Directory completed.
- Installation of the Digital Certificates completed.
- Wireless 802.1X service policy (3) completed.
- NAD integration completed.
- OnBoard Configuration for BYOD with basic configuration completed.
- Insight Configuration completed.
- Tests and validation of the service executed and documented.
- Knowledge transfer completed.
- All deliverables that are documents or reports, shall be considered as accepted when presented as described in the documentation review process of this document.
- Acceptance must include the signature of customer's Project Manager in charge of this project.

Eom

Solution testing & tuning in five (5) schools

Build an environment to perform updates, configuration and testing of equipment interconnection, with these devices you will simulate the client network, creating a similar environment, taking into account the configuration parameters generated in the solution plan and design.

CLARO PR will setup a five (5) schools pilots with an environment to tests system and equipment interconnection to simulate a common school setup.

Prerequisites

Before CLARO PR can perform the Services, DoE PR must comply with the following prerequisites:

- Assign a primary contact who is

– Responsible for all DoE Puerto Rico aspects of this SOW

– Authorized to make decisions relative to the SOW, including identification and assignment of DoE Puerto Rico resources

– Authorized to approve changes to the SOW

- DoE PR must certify in writing that the schools to be visited have electricity and links up and running, prior to the visit.
- DoE PR will inform in writing the schools to be installed.

Proof of Concept (PoC)

A real deployment of five (5) Schools at San Juan area will be performed.

The configurations on the Aruba Central must have been performed.

This stage is used as a validation of the developed design and will serve as a model for the rest of the sites.

On this stage CLARO PR will also define the details of parameters to be configured on the rest devices and, if necessary, affine the configured parameters at the Aruba Central.

PoC Review & Approval

CLARO PR should review the Proof of Concept functionality and provide a written approval in order to proceed with the full configuration and deployment. The PoC should be finalized before continuing with further phases.

Deliverables

- Milestone Plan.
- Document Templates.
- High Level Design document (HLD) for five (5) Schools Pilots
- Low Level Design document (LLD) for five (5) Schools Pilots
- Installation and configuration of APs for five (5) Schools Pilots
- Aruba Central Installed and configured for five (5) Schools Pilots.
- Clearpass Installed and configured for five (5) Schools Pilots.
- Prove of concept for five (5) schools.
- Testing plan protocol.

Acceptance Criteria

The team of CLARO PR will define formats and the protocol to be used which best suited to both parties.
Compliance of deliverables listed above.

- Milestone Plan or five (5) Schools Pilots accepted.
- Document Templates accepted.
- AP´s installed and configured for five (5) Schools Pilots
- Aruba Central Installed and configured for five (5) Schools Pilots
- Clearpass Installed and configured for five (5) Schools Pilots.
- Prove of concept for five (5) schools accepted.
- Testing Plan protocol executed and documented.
- All deliverables that are documents or reports, shall be considered as accepted when presented as described in the documentation review process of this document.
- Acceptance must include the signature of customer's Project Manager in charge of this project.

Installation and Configuration of APs

Prerequisites

Before CLARO PR can perform the Services, DoE PR must comply with the following prerequisites:

- Assign a primary contact who is

– Responsible for all DoE Puerto Rico aspects of this SOW

- Authorized to make decisions relative to the SOW, including identification and assignment of DoE Puerto Rico resources
- Authorized to approve changes to the SOW

- DoE Puerto Rico must certify in writing that the schools to be visited have electricity and links up and running, prior to the visit.
- DoE Puerto Rico will inform in writing the schools to be installed.

Deliverables

- Site Preparation.
- Pre-setting equipment.
- Document Templates
- Physical Installation and configuration of 70.000 APs provided by CLARO PR in table # 1.
- Testing plan protocol.
- Solution Stabilization.
- Knowledge transfer.
- AP´s tagging

Site preparation

The site preparation includes all activities required to make the site ready to implement the solution. Major activities include the inspection of the site, preparation and procurement. The following are the specific responsibilities during this phase:

CLARO PR will provide instructions to customer for the preparation of the site according to the so-called format.

The customer will complete the preparation of the site according to the formats and instructions supplied.

CLARO PR will coordinate a visit on site in order to collect information and carry out activities such as:

a. Racks or Space physical verification

b. Determine space for equipment installation

c. Needs wiring reorganization

d. Validate power appropriate for the equipment connection.

Pre-setting equipment

During this stage the customer will provide CLARO PR with all the information necessary to carry out the pre-setting and testing necessary to ensure the correct implementation of the equipment at the schools. This phase includes the following activities:

- Verification of inventory of the equipment which is part the proposed solution.
- Equipment power on to ensure correct operation of the Hardware.
- Connectivity verification according to the topology specified in the planning and design phase.
- Review of equipment operating system, basic configuration and connectivity
- Configuration parameters of the system according to the information provided by the client in the planning and design phase.
- CLARO PR will configure the equipment using as base the documents, minutes discussed and agreed upon information gathering phase.

Physical Installation and configuration

At this stage of the project, CLARO PR will implement the proposed network solution during the mutually agreed maintenance window. This phase includes the installation, configuration of the equipment and the verification of the functionality according to customer requirements specified during the planning phase of the project. During this phase CLARO PR would adjust and perform fine tuning if necessary.

The hardware in scope is defined in this "Table # 1". CLARO PR will only be liable for the configuration of equipment defined in this list.

The installation and configuration consist of the following task:

- Upgrade to latest most stable version.
- Interconnect all wireless equipment in the customer network.
- Assign Management IP Address to all equipment.
- Configure Wireless VLANs according wireless network design.
- Configure SSID's according wireless network design.
- AP Identification (Name, Location, Profile, MAC Address).
- Test AP's integration.
- Test authentication and connectivity.
- AP´s tagging.

The responsibilities within this phase include, but they are not limited to:

1. CLARO PR will make the necessary settings on the hardware, to comply with the requirements of the customer, according to the information provided in the solution plan and design phase.

2. The Client in conjunction with CLARO PR, will conduct a functional test defined and in accordance with the test plan previously approved in the project plan.

3. CLARO PR will provide engineering resources to carry out the activities necessary in this stage.

Eom

4. CLARO PR will provide a knowledge transfer session related to the specific works made at the End-Customer regarding the solution who will be

5. Once the Project Plan is completed, the initial timetable will be designed to perform work in mutually agreed maintenance windows.

Testing plan protocol

Once executed the configurations and implementation phases of the solution, there will be performance tests of the services in accordance with the test plan contained in the implementation plan. The execution of these tests may be total or partial, after the completion of each module configuration or after the full configuration of the proposed solution. These tests are related to the configurations of the equipment as indicated in the scope of the service and do not include any other platform, service or application that is associated with other elements present in the customer's network. These tests as a whole may not exceed 2 business days.

Solution stabilization

CLARO PR additionally offers to the customer, the service of a resource to perform troubleshooting tasks associated with the stabilization of the solution for a period of (2) days after the full implementation of the solution, physically at one of the facilities of the client (who must provide the space and tools necessary for the successful development of their activities) during this period the resource will be doing problems resolution with IP connectivity problems.

Acceptance Criteria

The team of CLARO PR will define formats and the protocol to be used which best suited to both parties.

Compliance of deliverables listed above.

- Site Preparation completed.
- Pre-setting equipment completed.
- Document Templates accepted.
- AP´s installed and configured showed in table # 1.
- Testing Plan protocol executed and documented.
- Knowledge transfer completed.
- AP´s tagging completed.
- All deliverables that are documents or reports, shall be considered as accepted when presented as described in the documentation review process of this document.
- Acceptance must include the signature of customer's Project Manager in charge of this project.

Support Services by 3 years

Deliverables

- Three (3) years of support.
- 8 x 5 coverage Schools and NIF - Monday to Friday School hours. Exception might apply upon request.
- Next Business Day for onsite support according to CLARO PR Hardware Support Service Document
- Hardware and firmware support

Major activities included in the service:

- Hardware onsite support
- Backup configurations
- Escalation management

How to get Support

If the customer experiences a service problem, a call must be placed to the PRT/Claro response center (787) 729-3131. On the call an onsite a ticket number will be provided to CLARO´s C-NOC. The engineer will first attempt to identify, remedy, and solve the problem remotely with the client on the call, prior to dispatching a technician.

Hardware onsite support

In the event a technical problem occurs in the hardware which cannot be resolved remotely, an PRT technician will be dispatched on site to provide services on hardware products and restore to its proper operation. PRT may decide to replace any faulty products rather than repairing them.

Backup configurations

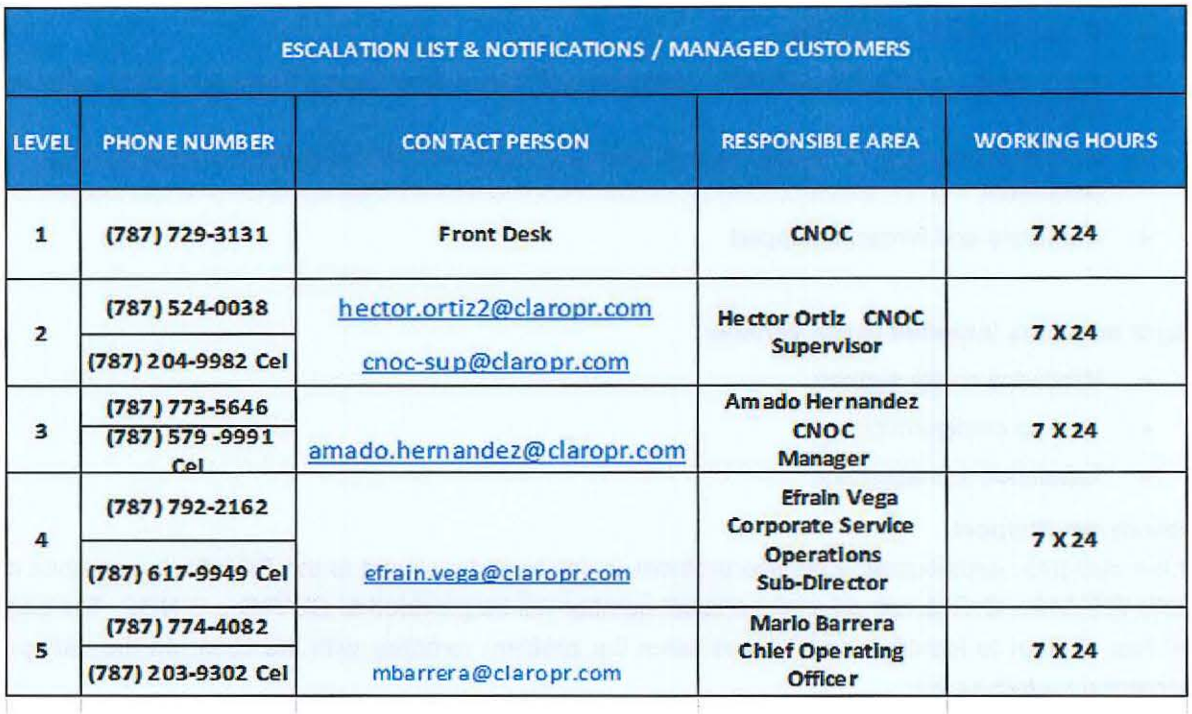
PRT included the service to back up and restore the configuration of each device in scope of this solution and project.

Business hours: Monday to Friday from 8:00 to 18:00 hours

Escalation management

PRT has established formal escalation procedures to facilitate the resolution of any problems. The local PRT management team coordinates problems scaling and defines resources from PRT and/or external (manufacture) or both necessary for the resolution of the problem.

Escalation list



ESCALATION LIST & NOTIFICATIONS / MANAGED CUSTOMERS				
LEVEL	PHONE NUMBER	CONTACT PERSON	RESPONSIBLE AREA	WORKING HOURS
1	(787) 729-3131	Front Desk	CNOC	7 X 24
2	(787) 524-0038 (787) 204-9982 Cel	hector.ortiz2@claropr.com cnoc-sup@claropr.com	Hector Ortiz CNOC Supervisor	7 X 24
3	(787) 773-5646 (787) 579 -9991 Cel	amado.hernandez@claropr.com	Amado Hernandez CNOC Manager	7 X 24
4	(787) 792-2162 (787) 617-9949 Cel	efrain.vega@claropr.com	Efrain Vega Corporate Service Operations Sub-Director	7 X 24
5	(787) 774-4082 (787) 203-9302 Cel	mbarrera@claropr.com	Mario Barrera Chief Operating Officer	7 X 24

Contact Information:	
Account Executive:	Arnaldo Diaz
Email Address	adiaz@PRTpr.com
Telephone Number	(787) 706-4706
Fax Number	(787) 792-8466
Technical Support:	Ing. Luis Bou
Email Address	lbou@Claropr.com
Telephone Number	(787) 273-4841
Sales Manager:	Lydia Toledo
Email Address	Claropr.comltoledo@Claropr.com
Telephone Number	(787) 273-4696

PRT key personnel assign to PRDE network and account management are:

Account Management

Mr. Arnaldo Diaz
Sales Account Executive
E-mail: adiaz@Claropr.com

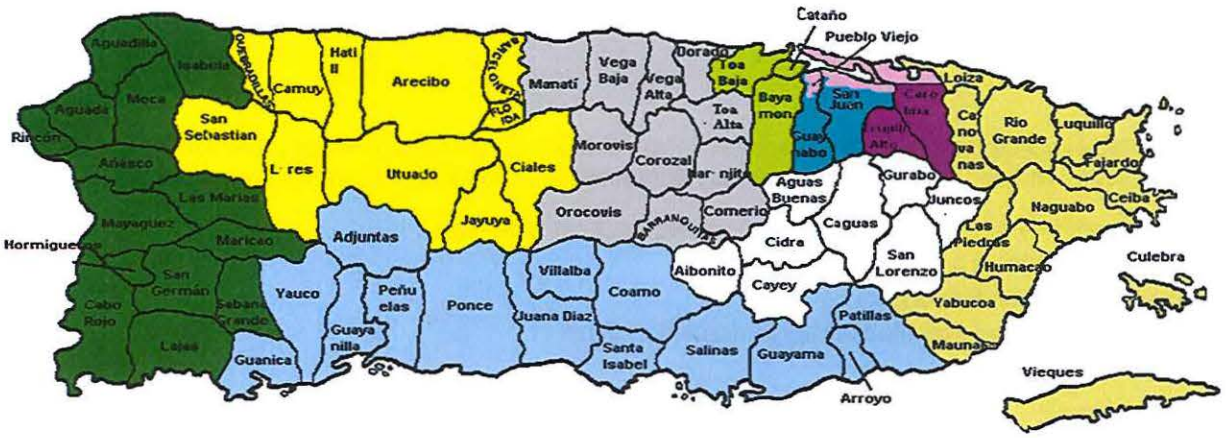
Technical Support

Eng. Luis Bou
Data Integrator Officer
E-mail: Lbou@Claropr.com

Manager Field Operation for Metro-Island

Departamento Servicios Operativos - 026		
METRO		
Nombre	Número Celular	Reporta a:
Carlos A. Román	385-9978	Ramón Maíz
Carlos I. Iglesias	384-9936	Ramón Maíz
Miguel Arce	375-9952	Ramón Maíz
Ángel Arce	391-9944	Ramón Maíz
José F. Mayoral	380-0497	Ramón Maíz
Jesús García	318-9953	Ramón Maíz
Francisco Rodríguez	382-7197	Ramón Maíz
Luis A. Vega Nolla	318-9917	Ramón Maíz
Elvín González	201-9289	Ramón Maíz
Ramón Maíz	**380-9955**	**Efraín Vega Acevedo**

ISLA		
Nombre	Número Celular	Reporta a:
Ángel M. Rivera	319-9975	Félix Daniel González
Efraín Martínez	318-1739	Félix Daniel González
Fernándo Cintrón	375-9937	Félix Daniel González
Fernando Rijos	375-9968	Félix Daniel González
Edgar Net	312-9967	Félix Daniel González
Juan Ponce de León	319-9922	Félix Daniel González
Luis Negrón	317-9987	Félix Daniel González
Oscar Alvarado	382-7419	Félix Daniel González
Víctor R. Vélez	201-8373	Félix Daniel González
Wilfredo Soto	315-9949	Félix Daniel González
Félix Daniel González	**315-9988**	**Efraín Vega Acevedo**



Victor Rivera	🟥	Orlando Cruz Serrano	🟨
Felix Rodriguez	🟩	Jesus Hernandez	⬜
Francisco J. Olivo	🟦	Waldemar Vélez	🟦
Ismael Ferrer	🟪	Maribel Gonzalez	🟨
Jose Asencio	🟩	Orlando Cruz/Félix Rodrg.	⬛

Acceptance Criteria

The team of CLARO PR will define formats and the protocol to be used which best suited to both parties. Compliance of deliverables listed above.

- Three (3) years of support completed and accepted.
- Hardware and firmware support completed and accepted.
- All deliverables that are documents or reports, shall be considered as accepted when presented as described in the documentation review process of this document.
- Acceptance must include the signature of customer's Project Manager in charge of this project.

Eom

Project Management

Project Manager

CLARO PR will designate a project manager ("Project Manager") to oversee the project, manage CLARO PR resources, and be the Customer's primary contact with CLARO PR regarding the following:

- Management of scope (formal or informal requests for changes)
- Conducting Status Meetings
- Preparing Status Reports
- Other activities as specified in this Statement of Work

Status Reports

Project Status Reports will be prepared by the CLARO PR Project Manager for review and discussion at the Status Meeting. Status Reports will contain the following:

- Project Status Summary
- Schedule Status against the Project plan
- Significant Issues and Actions to be taken by CLARO PR and/or the Customer
- Significant Decisions at prior status meeting
- Significant risks and Actions to be taken by CLARO PR and/or the Customer

Status reports are deemed accepted upon delivery by CLARO PR to DoE PR.

Status Meetings

Project status meetings will be held, weekly or when mutually agree between both parties. DoE PR's project manager and CLARO PR Project Manager will represent their organizations at these meetings. Status meetings will include:

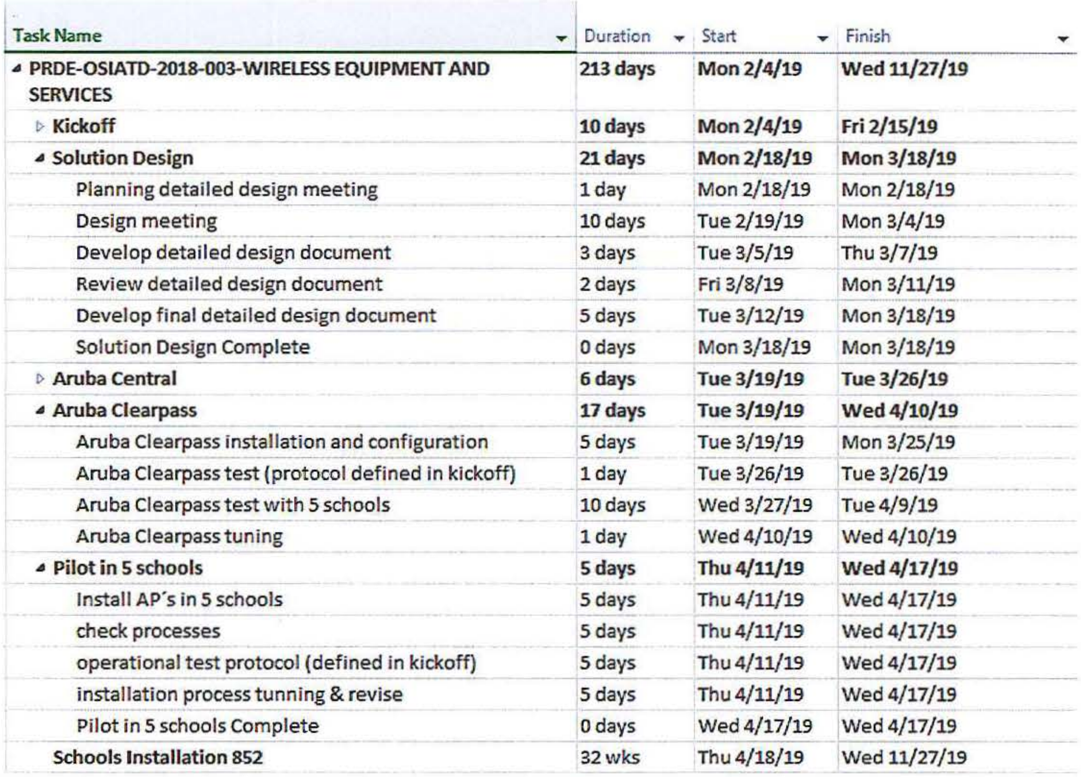
- Review of progress against schedule
- Review open Change Orders
- Review significant issues
- Review of significant risks
- Review achievement against milestones

Project Schedule

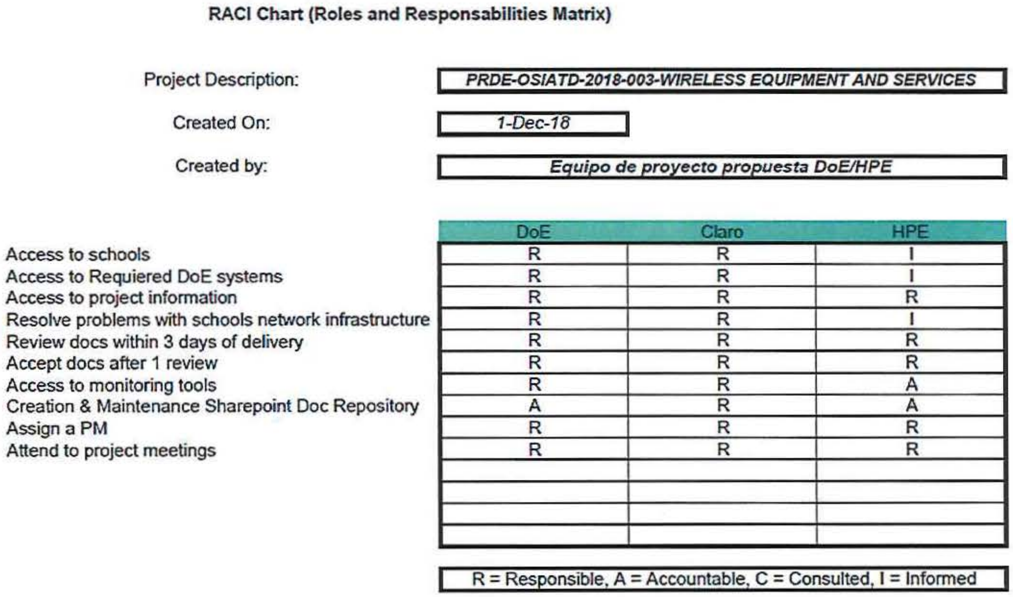
The CLARO PR Project Manager will create a Project Schedule that identifies and describes the activities and tasks required to provide the Services, Deliverables, and/or Configurations described. Significant changes (i.e., changes to the end date or an addition of hours to the project schedule) will be reviewed under the Change Management Process.

DoE PR will be responsible for reviewing and approving the contents of the initial version of the project schedule in accordance with the Document Review Process Once accepted, the project schedule will become the Project baseline against which Deliverables and performance of Services will be measured. Changes to the project schedule will be reviewed under the Change Process.

The following is a tentative schedule for the project. Dates shown on the schedule may change, depending on the start date of the project.



Task Name	Duration	Start	Finish
◢ **PRDE-OSIATD-2018-003-WIRELESS EQUIPMENT AND SERVICES**	**213 days**	**Mon 2/4/19**	**Wed 11/27/19**
▷ **Kickoff**	**10 days**	**Mon 2/4/19**	**Fri 2/15/19**
◢ **Solution Design**	**21 days**	**Mon 2/18/19**	**Mon 3/18/19**
Planning detailed design meeting	1 day	Mon 2/18/19	Mon 2/18/19
Design meeting	10 days	Tue 2/19/19	Mon 3/4/19
Develop detailed design document	3 days	Tue 3/5/19	Thu 3/7/19
Review detailed design document	2 days	Fri 3/8/19	Mon 3/11/19
Develop final detailed design document	5 days	Tue 3/12/19	Mon 3/18/19
Solution Design Complete	0 days	Mon 3/18/19	Mon 3/18/19
▷ **Aruba Central**	**6 days**	**Tue 3/19/19**	**Tue 3/26/19**
◢ **Aruba Clearpass**	**17 days**	**Tue 3/19/19**	**Wed 4/10/19**
Aruba Clearpass installation and configuration	5 days	Tue 3/19/19	Mon 3/25/19
Aruba Clearpass test (protocol defined in kickoff)	1 day	Tue 3/26/19	Tue 3/26/19
Aruba Clearpass test with 5 schools	10 days	Wed 3/27/19	Tue 4/9/19
Aruba Clearpass tuning	1 day	Wed 4/10/19	Wed 4/10/19
◢ **Pilot in 5 schools**	**5 days**	**Thu 4/11/19**	**Wed 4/17/19**
Install AP´s in 5 schools	5 days	Thu 4/11/19	Wed 4/17/19
check processes	5 days	Thu 4/11/19	Wed 4/17/19
operational test protocol (defined in kickoff)	5 days	Thu 4/11/19	Wed 4/17/19
installation process tunning & revise	5 days	Thu 4/11/19	Wed 4/17/19
Pilot in 5 schools Complete	0 days	Wed 4/17/19	Wed 4/17/19
Schools Installation 852	32 wks	Thu 4/18/19	Wed 11/27/19



RACI Chart (Roles and Responsabilities Matrix)

Project Description: *PRDE-OSIATD-2018-003-WIRELESS EQUIPMENT AND SERVICES*

Created On: *1-Dec-18*

Created by: *Equipo de proyecto propuesta DoE/HPE*

	DoE	Claro	HPE
Access to schools	R	R	I
Access to Requiered DoE systems	R	R	I
Access to project information	R	R	R
Resolve problems with schools network infrastructure	R	R	I
Review docs within 3 days of delivery	R	R	R
Accept docs after 1 review	R	R	R
Access to monitoring tools	R	R	A
Creation & Maintenance Sharepoint Doc Repository	A	R	A
Assign a PM	R	R	R
Attend to project meetings	R	R	R

R = Responsible, A = Accountable, C = Consulted, I = Informed

Eom

Project plan Attached:

PROPOU~1.MPP

PERFORMANCE MEASUREMENT AND REPORTING

A SharePoint will be generated with the following folder structure:

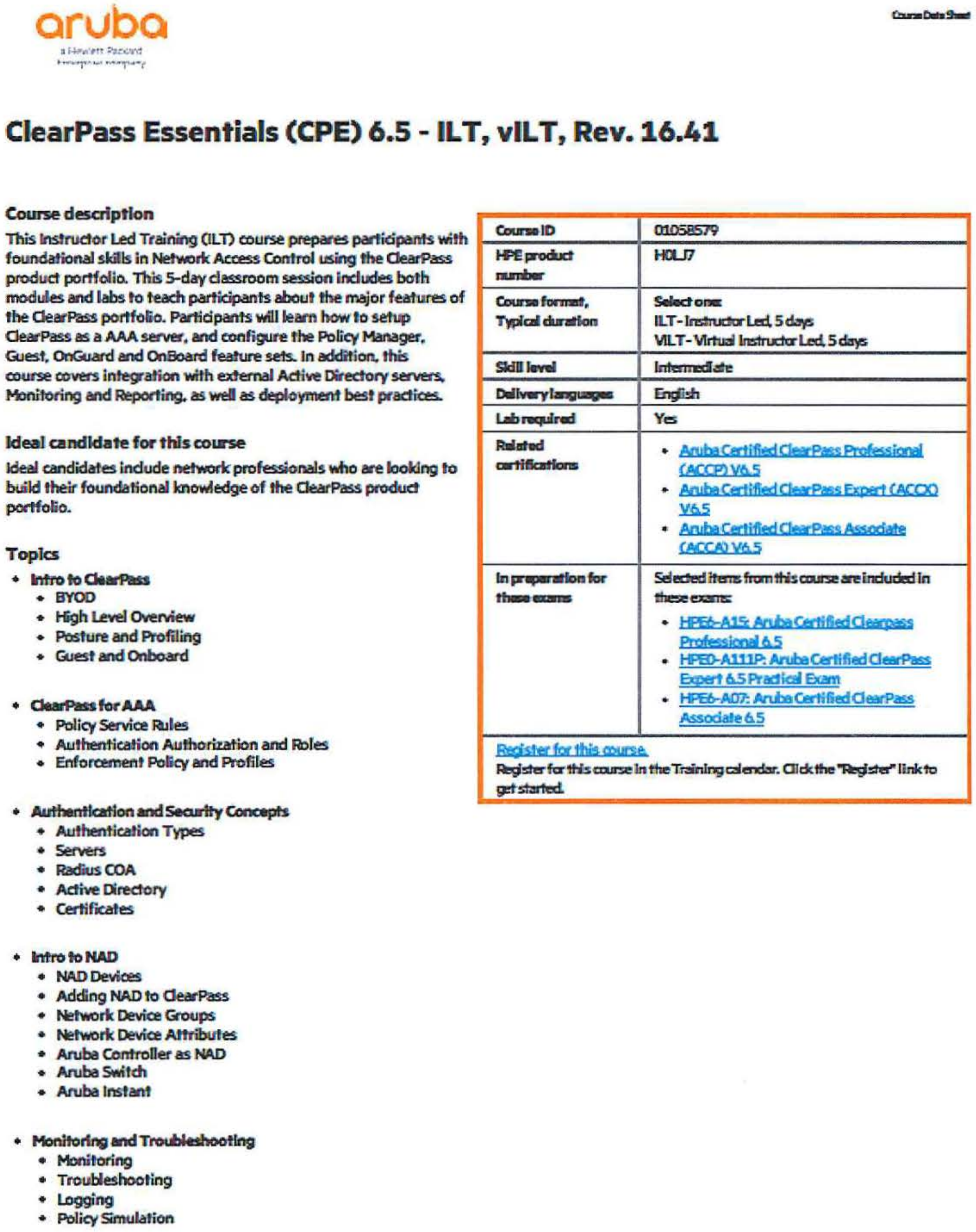
- Schools to work
- Schools in process
- Installed APs Schools
- Schools accepted
- Closed schools

Each school will have a particular folder:

- School Network point installation Map-DoE
- Test protocol results after installation
- Acceptance by clear of the test protocol
- DoE's acceptance of the test protocol

Training

To be successfully with management of the Wireless Network, PRTC/Claro and in fully compliant of the requirements of the RFP, we presented to the Department of Education all the trainings available for 12 (twelve) resources.



aruba
a Hewlett Packard Enterprise company

Course Data Sheet

ClearPass Essentials (CPE) 6.5 - ILT, vILT, Rev. 16.41

Course description

This Instructor Led Training (ILT) course prepares participants with foundational skills in Network Access Control using the ClearPass product portfolio. This 5-day classroom session includes both modules and labs to teach participants about the major features of the ClearPass portfolio. Participants will learn how to setup ClearPass as a AAA server, and configure the Policy Manager, Guest, OnGuard and OnBoard feature sets. In addition, this course covers integration with external Active Directory servers, Monitoring and Reporting, as well as deployment best practices.

Ideal candidate for this course

Ideal candidates include network professionals who are looking to build their foundational knowledge of the ClearPass product portfolio.

Topics

- Intro to ClearPass
  - BYOD
  - High Level Overview
  - Posture and Profiling
  - Guest and Onboard

- ClearPass for AAA
  - Policy Service Rules
  - Authentication Authorization and Roles
  - Enforcement Policy and Profiles

- Authentication and Security Concepts
  - Authentication Types
  - Servers
  - Radius COA
  - Active Directory
  - Certificates

- Intro to NAD
  - NAD Devices
  - Adding NAD to ClearPass
  - Network Device Groups
  - Network Device Attributes
  - Aruba Controller as NAD
  - Aruba Switch
  - Aruba Instant

- Monitoring and Troubleshooting
  - Monitoring
  - Troubleshooting
  - Logging
  - Policy Simulation

Course ID	01058579
HPE product number	H0LJ7
Course format, Typical duration	Select one: ILT - Instructor Led, 5 days VILT - Virtual Instructor Led, 5 days
Skill level	Intermediate
Delivery languages	English
Lab required	Yes
Related certifications	• Aruba Certified ClearPass Professional (ACCP) V6.5 • Aruba Certified ClearPass Expert (ACCX) V6.5 • Aruba Certified ClearPass Associate (ACCA) V6.5
In preparation for these exams	Selected items from this course are included in these exams: • HPE6-A15: Aruba Certified Clearpass Professional 6.5 • HPE0-A111P: Aruba Certified ClearPass Expert 6.5 Practical Exam • HPE6-A07: Aruba Certified ClearPass Associate 6.5

Register for this course.
Register for this course in the Training calendar. Click the "Register" link to get started.

- **ClearPass Insight**
  - Insight Dashboard
  - Insight Reports
  - Insight Alerts
  - Insight Search
  - Insight Administration
  - Insight Replication

- **Active Directory**
  - Adding AD as Auth Source
  - Joining AD domain
  - Using AD services

- **External Authentication**
  - Multiple AD domains
  - LDAP
  - Static Host Lists
  - SQL Database
  - External Radius Server

- **Guest**
  - Guest Account creation
  - Web Login pages
  - Guest Service configuration
  - Self-registration pages
  - Configuring NADS for Guest
  - Guest Manager Deep Dive
  - Web Login Deep Dive
  - Sponsor Approval
  - MAC Caching

- **Onboard**
  - Intro to Onboard
  - Basic Onboard Setup
  - Onboard Deepdive
  - Single SSID Onboarding
  - Dual SSID Onboarding

- **Profiling**
  - Intro to Profiling
  - Endpoint Analysis Deep Dive

- **Posture**
  - Intro to Posture
  - Posture Deployment Options
  - OnGuard Agent Health Collection
  - OnGuard workflow
  - 802.1x with Posture using Persistent/dissolvable agent
  - OnGuard web Login
  - Monitoring and Updates

- **Operation and Admin Users**
  - Operations
  - Admin Users

- **Clustering and Redundancy**
  - Clustering
  - Redundancy
  - LAB

- **Licensing**
  - ClearPass Licensing
  - Base License
  - Applications

- **Single Sign-On**
  - Deployment Options
  - ClearPass Admin Login SSO
  - Access Network SSO
  - ASO-Auto-Sign On
  - Configuration and Demo

- **ClearPass Exchange**
  - Intro
  - Examples
  - General HTTP Palo Alto Firewall
  - Configuration

- **Case Study**
  - Objectives
  - Discussion
  - Advanced Labs Overview

Objectives

After you successfully complete this course, expect to be able to:

- Ability to setup ClearPass as a AAA server
- Demostrate Configuration Guest, Ongurad, Onboard and Profiling features
- Integrate with External AD Server
- Understand Monitoring and Reporting
- Demostrate Scaling and deployment of best practices

How to register

View the Certification and Learning Global Training Calendar to register for the training offerings that best meets your needs.

Policies, fees and cancellations

Course fees may vary. Fees are established and collected by the training center that delivers the course. Cancellation fees may apply. Contact your HPE Authorized Training Partner for their respective policies.

For more information

Contact our program

© Copyright 2019 Hewlett Packard Enterprise. The information contained herein is subject to change without notice. The only warranties for HPE products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

Information is as of September 2017, Revision 4

Eom