SOLUTIONS GUIDE

GOVERNMENT

SEPTEMBER 2020

aruba
a Hewlett Packard
Enterprise company

TABLE OF CONTENTS

INTRODUCTION

The purpose of this section is to introduce the reader to the Government Solutions Guide and provide an overview of the wide variety of mobile networking infrastructure solutions that Aruba, a Hewlett Packard Enterprise company, can offer to the government customer.

Note to the Reader

The Aruba Government Solutions Guide provides an overview of Aruba's products and key characteristics and describes different use cases supported by a network powered by Aruba. It is focused on the network environment, needs and requirements of government organizations. This document may be read end-to-end, but the reader may find it beneficial to scan the table of contents and read the sections of the document that are deemed most relevant. This document does not communicate product specs like a datasheet or reference end-user case studies since existing documents from Aruba already provide this. This document is designed to be a reference guide, that brings together the relevant organizational, mission, application and technical information in one place in order to provide government network architects and administrators an answer to the question "what does Aruba do well and how can they best serve our organization?"

Aruba Government Solutions

Aruba is the leading provider of next-generation wireless network access solutions for the mobile enterprise – including secure wireless LAN (WLAN), remote access, outdoor mesh networks, guest access, classified networking and network solutions. Aruba is a general-purpose secure mobility networking infrastructure company, offering distributed networking solutions for many location-centric or application-centric networking requirements.

Aruba is the only enterprise WLAN solution vendor that is dedicated to helping government agencies and organizations build best-of-breed, highly secured, mobility-oriented networks. Aruba's solution differentiators are found within three key core competencies for robust WLAN implementations:

1. **Wireless and Mobility** – Aruba ensures optimal WLAN device and application performance through the development and deployment of highly tuned RF and mobility control systems.
2. **Fully Integrated Security** – Aruba understood from the beginning that centralized, end-to-end encryption, role-based access control and a stateful user-based firewall were required as integral components to the WLAN solution, thereby solving the dilemma between seamless mobility and security.
3. **Unified Solutions and Future-proofed Architecture** – With an Aruba mobility solution, organizations are not restricted to specific products for different deployment cases. Aruba's solutions can be used simultaneously for WLAN access, mesh, remote access and video surveillance. Aruba provides unified management of the entire WLAN architecture through our Mobility Controllers and our award-winning multi-vendor enterprise wireless management solution called AirWave. And, Aruba has a purpose-built systems architecture that delivers the horsepower needed for the mobility applications of today and tomorrow.

Aruba, through our integration partners, has deployed hundreds of ATO-validated and operating enterprise WLAN solutions within the Department of Defense (DoD), each operating hundreds to thousands of access points. Aruba is recognized as the only authorized enterprise WLAN solution provider within the US Air Force, and is only one of two approved enterprise WLAN vendors within the US Army and DoD Military Health System.

This Guide is comprised of the following sections:

- **Components:** Overview of Aruba's products and solution components.
- **Architecture:** Explanation of Aruba's unique architecture and benefits.
- **Locations and Topologies:** Depiction of the different types of physical deployment scenarios appropriate for an Aruba-based network, including physical and logical topological diagrams.
- **Use Cases and Solutions:** Outline of use cases typically found in the federal government sphere and discussion of Aruba solutions.
- **Technology Reference:** Summary list of Aruba standards, certifications and government validations.

ARUBA'S SECURE NETWORK ARCHITECTURE

This section contains a brief description of the components of the Aruba architecture and its concept of operations. The basic elements are the Aruba Mobility Controller (which runs ArubaOS), optional ArubaOS Software Modules, Aruba Access Points, AirWave Management System, ClearPass Policy Management System and Virtual Internet Access (VIA) client.

Mobility Controller

The Aruba Mobility Controller serves as the centralized control point for all network and user activity and is designed to address a wide range of wireless and wired network requirements such as mobility, security, policy management, and remote access for networks of any size. Unlike other solutions, Aruba WLAN systems are purpose-built and completely self-contained, and do not require ancillary security appliances or cryptology overlays. Running the ArubaOS operating system, Mobility Controllers support a library of base features and functionality as well as optional software modules including: Adaptive Radio Management, network access control, policy-enforcement per-user firewall, AppRF technology, FIPS 140-2 validated 802.11i, NSA Suite-B crypto termination, and wireless intrusion detection. In competing systems, this level of support requires separate dedicated appliances.

Figure 1: Aruba Mobility Controllers

Mobility Controllers feature programmable network processors and encryption engines that are optimized for 802.11a/b/g/n/ac data, voice, and video networks, providing high throughput, massive scalability, and advanced security. Controllers are typically installed in a secure data center near the application, servers and voice systems, or in the core network of a building. Controllers are compactly packaged, offer a range of high-availability options, and feature very low energy consumption to reduce ongoing operating expenses and HVAC loading. For scalability and redundancy, controllers can be logically connected together in a hierarchy. More information on the Aruba Mobility Controllers can be found on the Aruba website.

Key characteristics of the Aruba Mobility Controller include:

- Scalability from 1.6Gb/s to 30Gb/s of AES-CCMP-256 or AES-256-GCM encrypted packet throughput
- Models available for deployment in a secure Data Center, network core, or branch office
- Adaptive 802.11a/b/g/n/ac WLAN support
- IPSec/SSL VPN capabilities supporting NSA Suite-B algorithms, which are approved for use in transmission of classified information
- Easily deployed as an overlay without any change in the wired network
- Works in conjunction with ArubaOS and Aruba Access Points for many different WLAN deployment modes, including campus, mesh, point-to-point and remote
- Role-based access control with supporting security policies that can be applied to users, mobile devices, applications, and location
- Context awareness of mobile devices connected to the network
- FIPS-140-2 Level 2 Validated, Unified Capabilities Approved Products List (UC-APL) certified, Common Criteria Validated
- Meets DoD Directive 8100.2, 8500.1 and DoD Directive 8420.1 on WLAN solutions

ArubaOS

Powering the Aruba solution is ArubaOS®, which serves as the operating system and application engine for all Aruba Mobility Controllers and access devices. ArubaOS includes a base set of capabilities as well as optional software modules enabled through license keys for additional functionality. The software architecture of ArubaOS is designed for scalable performance and is built using three core components:

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

ArubaOS, running on the high-performance controller hardware, provides literally hundreds of features and capabilities, including:

- Network integration through L2 services (VLAN, RSTP, etc.) and L3 services (VRRP, OSPF, etc.)
- L2 and L3 secure user connectivity and mobility
- Centralized and/or distributed Wi-Fi and IPsec encryption (including NSA Suite-B)
- Network access control, role-based access control and user authentication system integration
- Common Criteria validated Policy Enforcement Firewall, identity-based and inter-group/intra-VLAN firewalling
- Adaptive Radio Management, providing dynamic wireless RF configuration and optimization
- Fair access policies and user traffic management, Quality of Service (QoS) control
- Wireless Intrusion Prevention
- Device identity capabilities through fingerprinting
- Visibility offered by AppRF technology allowing IT to see applications by user, prioritize them, and control access based on policies
- FIPS 140-2 Level 2/3 validation, Common Criteria Type-accreditation, Unified Capabilities Approved Product List
- ClientMatch technology that continuously steers clients to the optimum AP based on metrics and eliminates sticky clients and maximizes Wi-Fi performance
- Aruba's SDN API integration with Skype for Business provides full visibility to call quality and detailed call reporting

More information can be found on the Aruba website in the ArubaOS datasheet.

Access Points

Aruba's Access Points (APs) serve as secure on-ramps to aggregate wireless and wired user traffic to the enterprise network, transporting this traffic between users and the centralized mobility controller. Aruba has a comprehensive product line for many different deployment environments that may require support for:

- Single and Dual Radio 802.11a/b/g/n/ac Wave 2
- Wireless and wired networks
- Indoor and outdoor usage
- Telecommuter deployments
- Harsh environment and industrial applications
- Mesh and wireless bridging deployments
- Unclassified and classified environments

In addition to providing WLAN and wired network access, wireless access points provide RF monitoring services for both performance and security monitoring. All AP configuration and monitoring takes place from the controller; the intermediate Ethernet LAN or IP WAN requires no modifications for the AP to be deployed – there simply needs to be basic IP connectivity between the AP and the controller.

Depending on agency or department needs, any Aruba AP can easily be deployed in one of the following modes via the Controller:

- **Campus Mode**, where the AP is attached to one or more Ethernet connections (typically 802.3at PoE+) and valid user traffic is forwarded untouched from the WLAN to the backbone and vice-versa.
- **Mesh AP Mode**, where the AP is specifically configured to connect to the backbone by transparently and securely bridging traffic via a WLAN point-to-point connection to another AP.
- **Remote AP Mode**, where the AP performs additional traffic management functions to connect the users across a lower-speed, higher-latency IP WAN of any type. All traffic is IPsec encrypted using government-validated algorithms between the AP and the Controller, further enhancing the communications security posture of the environment.

Figure 2: Aruba Access Points

	310 Series	325 Series
5 GHz radio	4x4:43:3	4x4:3:3
2.4 GHz radio	2x2:2	4x4:4
VHT 160 Support	yes (2x2)	no
Built-in BLE	yes (2x2)	yes
Size	162mm x 180mm x48mm	203mm x 203mm x57mm
Weight	650g	950g

Figure 3: 310/320/330 Series Feature Matrix Summary

Aruba's new series of 802.11ac Wave 2 access points support multi-user MIMO to boost network efficiency. Wave 2 access points include the 300, 310, 320, and 330 series to match every need. All series are available with integrated omni-directional or external antenna options.

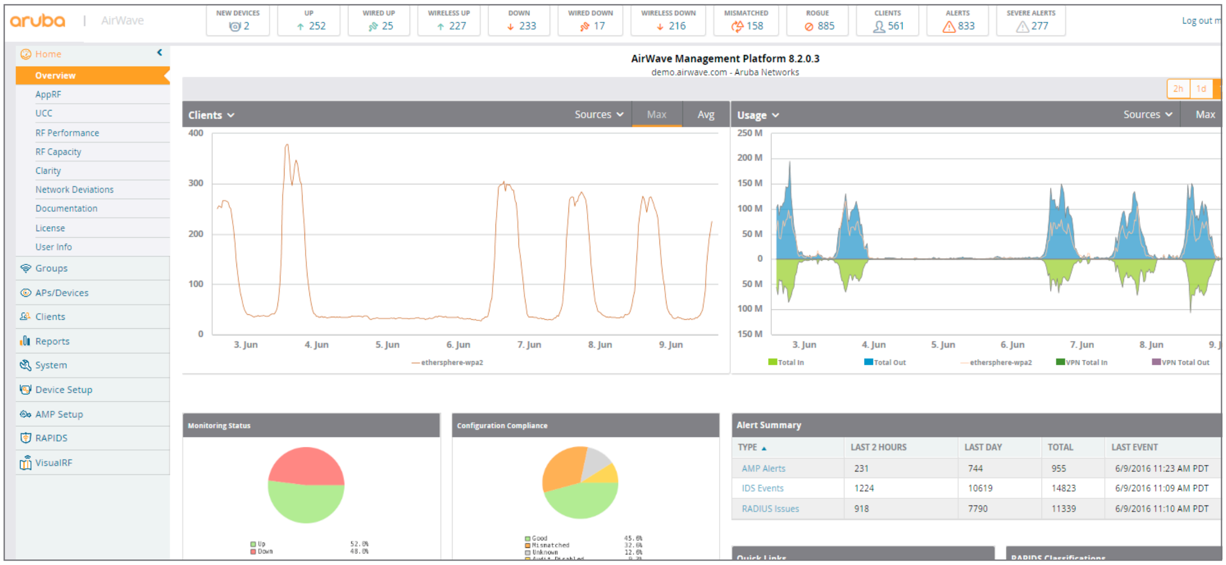
More information on Aruba Access Points can be found on the Aruba website.

AirWave Management System

Aruba's AirWave Management System is a multi-vendor network operations solution for wired and wireless infrastructure as well as mobile devices, eliminating the need for multiple, single-purpose management tools. Available as either installable software or an appliance, AirWave enables the IT service desk to triage connectivity issues as well as providing a simpler way to enforce policies and actionable information.

The AirWave Wireless Management System delivers streamlined management, IDS security, and enhanced visibility using the following:

1. **AirWave Management Platform (AMP):** AirWave Management Platform, the core component of AirWave, provides efficient, centralized management of wireless infrastructure and visibility across the wired edge of the network. It communicates with and controls the wireless infrastructure via standard protocols (SNMP, HTTPS, and so on) across a LAN or WAN. It provides an easy-to-use web-based interface that gives people across the IT organization a personalized view of the network with administrative privileges tailored to their specific job responsibilities.



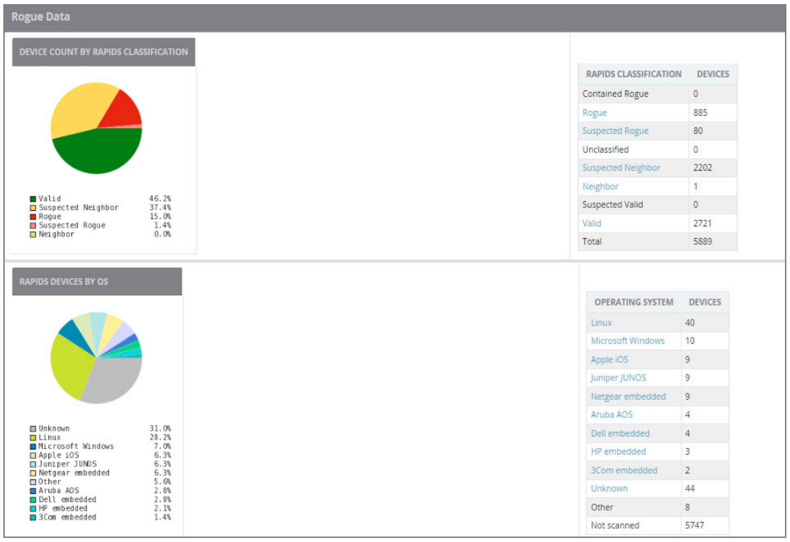
Alert Summary

TYPE ▲	LAST 2 HOURS	LAST DAY	TOTAL	LAST EVENT
AMP Alerts	231	744	955	6/9/2016 11:23 AM PDT
IDS Events	1224	10619	14823	6/9/2016 11:09 AM PDT
RADIUS Issues	918	7790	11339	6/9/2016 11:10 AM PDT

Figure 4: AirWave Management Platform

2. **AirWave RAPIDS™ Rogue Detection:** AirWave RAPIDS automatically detects and locates unauthorized access points through a patented combination of wireless and wired network scans. The RAPIDS software uses existing, authorized APs to scan the RF environment for any unauthorized devices in range; it also scans the wired network to determine whether any unknown devices are connected. RAPIDS then correlates all of this data and uses a set of rules to highlight only those devices that are truly a threat to the organization, greatly reducing false-positives. It also captures and manages IDS events. RAPIDS improves network security, manages compliance requirements, and reduces the cost of manual security efforts.

3. **AirWave VisualRF™ Location and Mapping:** AirWave VisualRF provides an accurate view of the entire network. It automatically generates a map of the RF environment and the underlying wired uplinks topology, showing a full view of what the network looks like — in real time. VisualRF uses RF measurements gathered from active wireless access points and controllers, without the need for a costly, separate location appliance.



🟩 Valid	46.2%
🟨 Suspected Neighbor	37.4%
🟥 Rogue	15.0%
🟥 Suspected Rogue	1.4%
🟩 Neighbor	0.0%

RAPIDS CLASSIFICATION	DEVICES
Contained Rogue	0
Rogue	885
Suspected Rogue	80
Unclassified	0
Suspected Neighbor	2202
Neighbor	1
Suspected Valid	0
Valid	2721
Total	5889

⬜ Unknown	31.0%
🟩 Linux	28.2%
🟦 Microsoft Windows	7.0%
🟩 Apple iOS	6.3%
🟦 Juniper JUNOS	6.3%
🟨 Netgear embedded	6.3%
🟪 Other	5.6%
🟦 Aruba AOS	2.8%
🟩 Dell embedded	2.8%
🟦 HP embedded	2.1%
🟦 3Com embedded	1.4%

OPERATING SYSTEM	DEVICES
Linux	40
Microsoft Windows	10
Apple iOS	9
Juniper JUNOS	9
Netgear embedded	9
Aruba AOS	4
Dell embedded	4
HP embedded	3
3Com embedded	2
Unknown	44
Other	8
Not scanned	5747

Figure 5: AirWave RAPIDS™ Rogue Detection

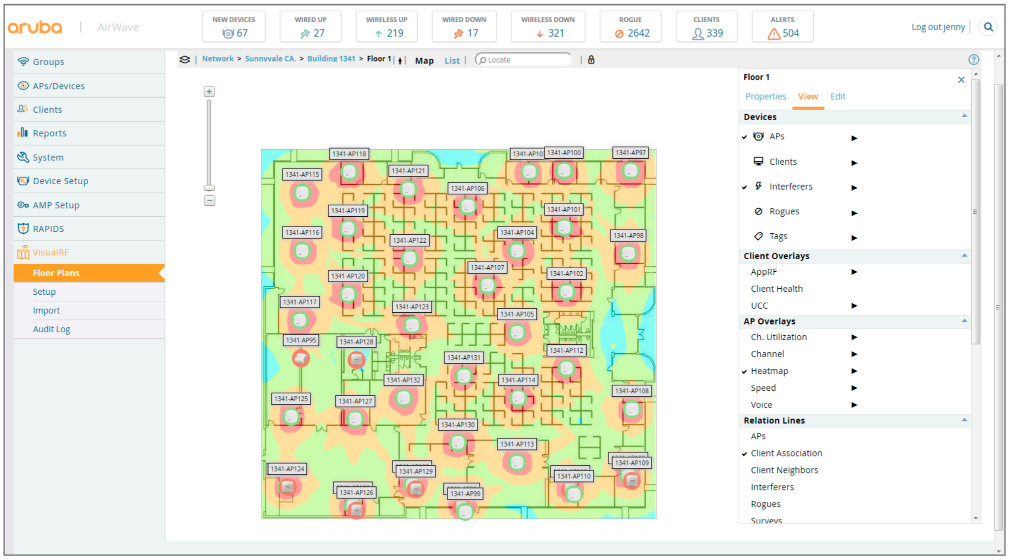
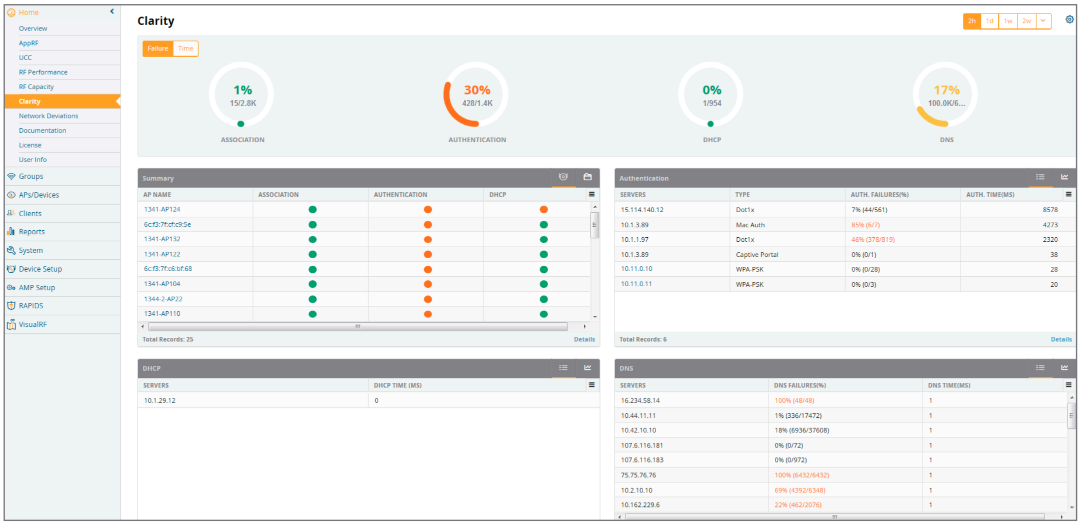


Figure 6: AirWave VisualRF™ Location and Mapping

4. **AirWave Clarity Provides End-to-end Visibility:** Clarity enables visibility into non-RF metrics – not only giving end-to-end visibility into a wireless user experience – but also the ability to foresee connectivity issues before users are even impacted. Live user monitoring lets IT proactively monitor live client data flow and visualize radio association, authentication, DHCP and DNS service response times and failure rates.

5. **AppRF Dashboards** provide deep visibility into common applications and web traffic on the network to ensure mission-critical apps get priority, users are off risky sites, or for simply gauging usage patterns. With AirWave, AppRF statistics are recorded for the entire network and presented in a clean and easy to use dashboard. Whether needing a high level overview or drilling down into the details, it all takes just a few clicks.



Clarity

1% 15/2.8K ASSOCIATION

30% 428/1.4K AUTHENTICATION

0% 1/954 DHCP

17% 100.0K/6... DNS

Summary

AP NAME	ASSOCIATION	AUTHENTICATION	DHCP
1341-AP124	●	●	●
6c:f3:7f:cf:c9:5e	●	●	●
1341-AP132	●	●	●
1341-AP122	●	●	●
6c:f3:7f:c6:bf:68	●	●	●
1341-AP104	●	●	●
1344-2-AP22	●	●	●
1341-AP110	●	●	●

Total Records: 25 Details

Authentication

SERVERS	TYPE	AUTH. FAILURES(%)	AUTH. TIME(MS)
15.114.140.12	Dot1x	7% (44/561)	8578
10.1.3.89	Mac Auth	85% (6/7)	4273
10.1.1.97	Dot1x	46% (378/819)	2320
10.1.3.89	Captive Portal	0% (0/1)	38
10.11.0.10	WPA-PSK	0% (0/28)	28
10.11.0.11	WPA-PSK	0% (0/3)	20

Total Records: 6 Details

DHCP

SERVERS	DHCP TIME (MS)
10.1.29.12	0

DNS

SERVERS	DNS FAILURES(%)	DNS TIME(MS)
16.234.58.14	100% (48/48)	1
10.44.11.11	1% (336/17472)	1
10.42.10.10	18% (6936/37608)	1
107.6.116.181	0% (0/72)	1
107.6.116.183	0% (0/972)	1
75.75.76.76	100% (6432/6432)	1
10.2.10.10	69% (4392/6348)	1
10.162.229.6	22% (462/2076)	1

Figure 7: AirWave Clarity

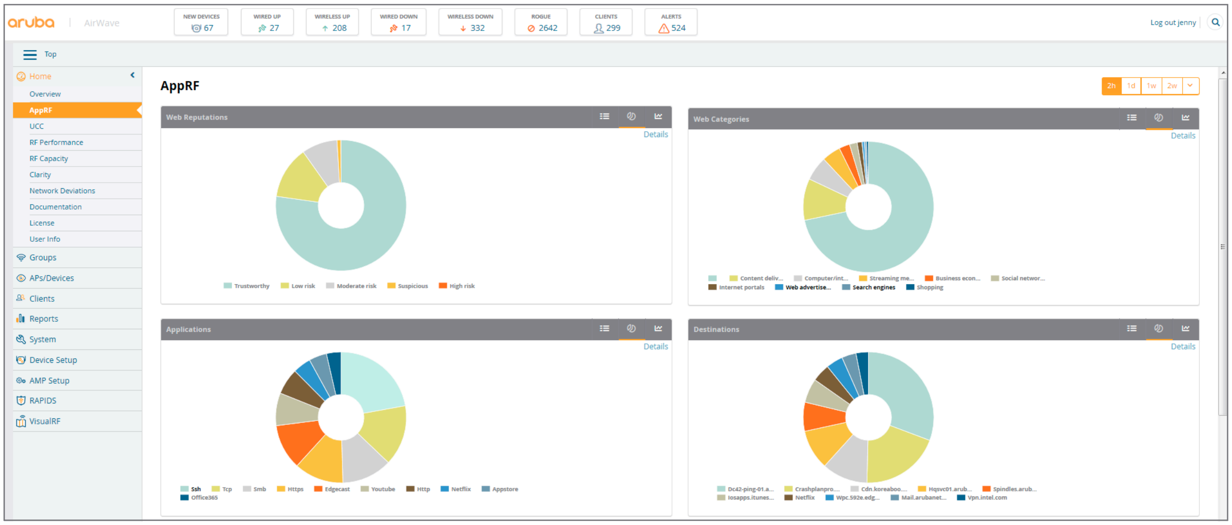


Figure 8: AppRF Dashboards

6. **UCC Dashboards** provide an aggregated view of the Unified Communication and Collaboration (UCC) calls made in the network. Charts display trending information for UCC call volume, quality and clients. Network administrators see a top level view of the call quality assessment, and can further drill down into a specific view based on the analysis required. Call quality is encapsulated into an Aruba proprietary metric called UCC score. The UCC score for voice and video calls is measured by taking into account the following metrics:
   - Delay
   - Jitter
   - Packet Loss

ClearPass Access Management System

Aruba's ClearPass Access Management System is a multi-vendor, standards-based secure network access solution that provides access and policy control across an agency's wired, wireless, and VPN networks. Designed to be implemented as an overlay solution with an existing network, ClearPass is seamlessly integrated to leverage the existing network, identity, and security infrastructure. ClearPass is FIPS compliant and has Common Criteria validation. In addition, it supports Suite-B digital certificates for authentication of Commercial Solutions for Classified (CSfC) deployments.

ClearPass automates user and device access, policy management, and the provisioning of devices for secure network access and posture assessment. This ensures that each user has the correct access privileges depending upon who they are and on which devices they authenticate. Devices running Windows, MacOS, iOS, Android, and Linux can all be managed through ClearPass.

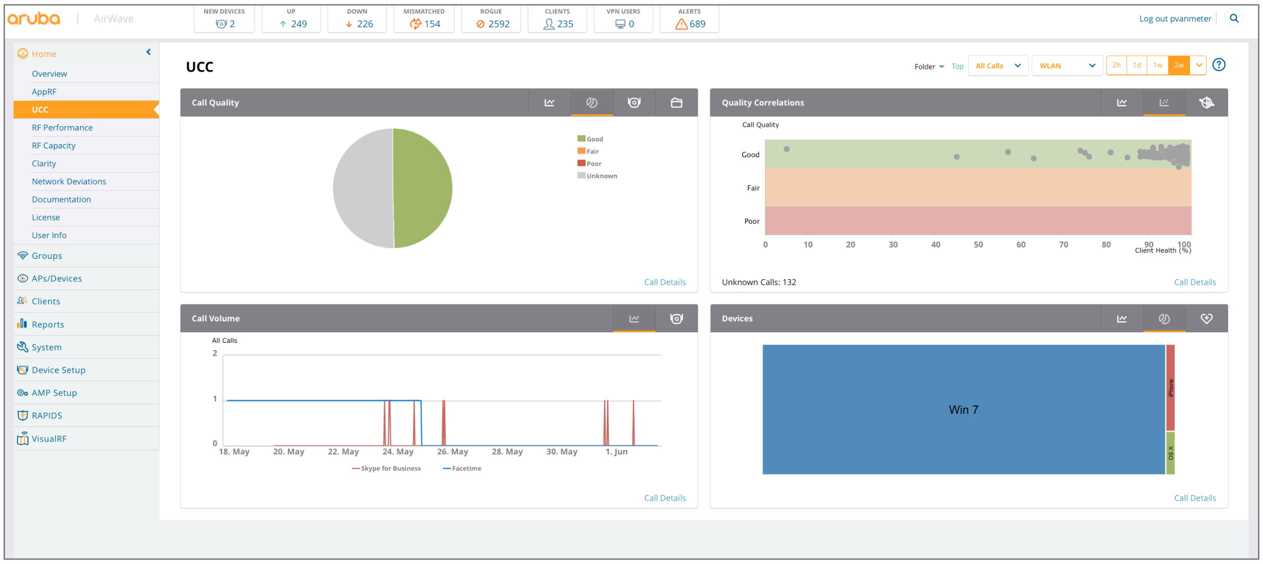
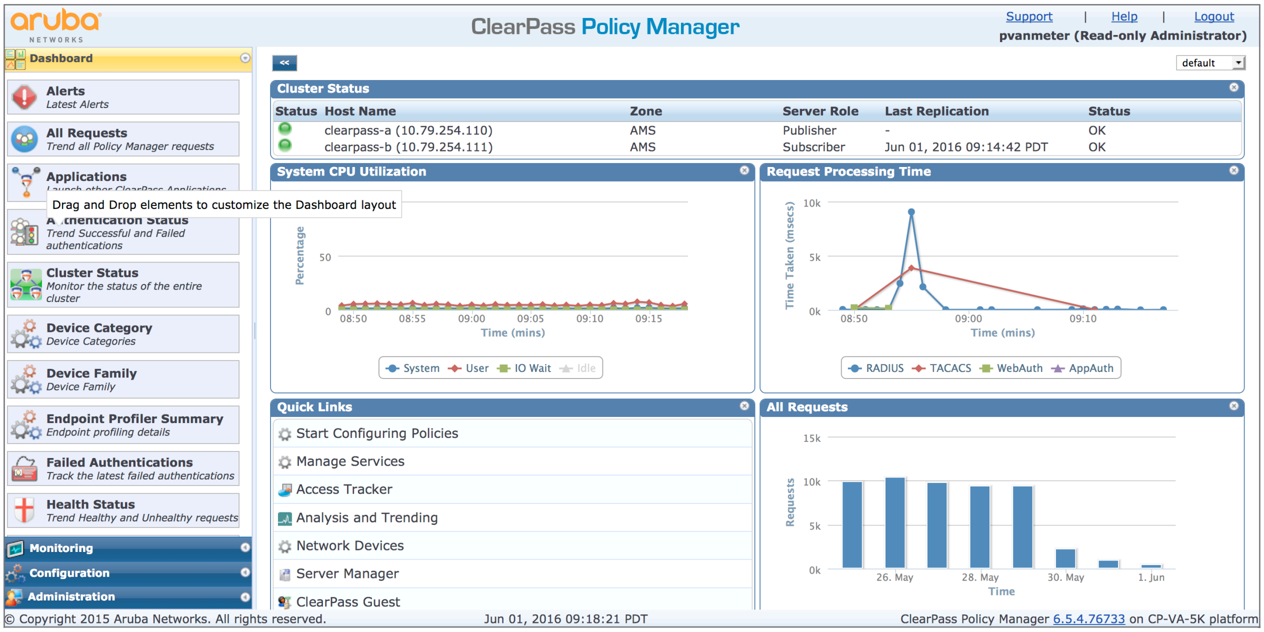


Figure 9: UCC Dashboards

Aruba ClearPass is available as a hardware or virtual appliance, supporting tens of thousands of users and devices. The ClearPass platform consists of the following modules:

- **Policy Management:** Included as part of the ClearPass Management System, the Policy Manager is the central policy enforcement decision point. In a single platform, ClearPass can perform mobile application and device management, device onboarding and management, device health monitoring and guest access. The Policy Manager provides integrated RADIUS and TACACS+ capabilities for AAA, along with authentication support for Microsoft Active Directory, LDAP, SQL and Kerberos authentication databases. As users and devices authenticate to the network, user and endpoint access policies are enforced, providing true context-based access control. Additional features include differentiated access based on a variety of attributes, such as user role, device, time, and location, along with device registration and profiling, endpoint health assessments and reporting.
- **Device Onboarding and Management:** This add-on module automates 802.1X configuration for IT-managed devices, such as Windows, Mac OSX, iOS and Android, across wired, wireless and VPN networks. For agencies that anticipate the influx of a large number of these devices, the configuration of 802.1X device authentication can be accomplished through an automated provisioning process. For those agencies that support BYOD, the same automated provisioning process can be utilized to allow these devices onto the network. Additional features include the ability to push required applications and configuration settings for mobile email with Exchange ActiveSync and VPN clients for some device types.
    - ClearPass QuickConnect: Built-into Device Onboarding and Management, this cloud-based service provides users the ability to perform self-service 802.1X configuration capabilities to support 802.1X authentication on wired and wireless networks for Windows, Mac OSX, iOS and Android devices. QuickConnect streamlines device configuration for IT and end-users by presenting a configuration wizard through the use of a captive portal, Active Directory group policy object, or CD. The user authenticates through the portal, runs through the wizard, and provides the overall configuration to be implemented onto the device.



ClearPass Policy Manager

Support | Help | Logout
pvanmeter (Read-only Administrator)

Dashboard

- Alerts – Latest Alerts
- All Requests – Trend all Policy Manager requests
- Applications – Launch other ClearPass Applications
- Authentication Status – Trend Successful and Failed authentications
- Cluster Status – Monitor the status of the entire cluster
- Device Category – Device Categories
- Device Family – Device Family
- Endpoint Profiler Summary – Endpoint profiling details
- Failed Authentications – Track the latest failed authentications
- Health Status – Trend Healthy and Unhealthy requests

Monitoring
Configuration
Administration

Drag and Drop elements to customize the Dashboard layout

Cluster Status

Status	Host Name	Zone	Server Role	Last Replication	Status
●	clearpass-a (10.79.254.110)	AMS	Publisher	-	OK
●	clearpass-b (10.79.254.111)	AMS	Subscriber	Jun 01, 2016 09:14:42 PDT	OK

System CPU Utilization

Request Processing Time

Quick Links

- Start Configuring Policies
- Manage Services
- Access Tracker
- Analysis and Trending
- Network Devices
- Server Manager
- ClearPass Guest

All Requests

© Copyright 2015 Aruba Networks. All rights reserved. Jun 01, 2016 09:18:21 PDT ClearPass Policy Manager 6.5.4.76733 on CP-VA-5K platform

Figure 10: ClearPass Policy Management System

- **Device Health:** These software agents perform advanced endpoint posture assessments to minimize the risk of viruses and misuse of applications before devices are allowed on the network. The device health module provides support for verifying the presence of anti-virus, anti-spyware, and firewall software from more than 80 vendors. In addition, it checks for allowable services, processes, peer-to-peer applications such as Skype, USB storage devices, VM clients, hotspots, etc. Agents exist for Windows, Mac OSX and Linux.
- **Guest Access:** For those agencies that desire support for guest access, the ClearPass Guest Access module enables various agency personnel to manage guest Wi-Fi accounts. Please see page 34 for more details.

Aruba Virtual Intranet Access Client

The Virtual Intranet Access (VIA) client is part of the Aruba remote networks solution targeted for mobile users, tablets, smartphones, and laptops. VIA detects the user's network environment as either trusted or un-trusted. VIA automatically scans and selects the best secure connection to the enterprise network. Trusted networks typically refer to a protected enterprise network that allows users to directly access network resources. Un-trusted networks are outside public areas such as airports, hotels, home networks, etc. When VIA detects that it is on an un-trusted network, the client launches a secure IPSec or SSL connection to the enterprise network to allow access to network resources. VIA can function automatically off of Wi-Fi, wired, and even 3G/4G cellular networks.

VIA provides a zero-touch end user experience by automatically configuring and also determining when to establish a secure IPSec or SSL connection back to the enterprise network without requiring any user intervention. Because the VIA client communicates to an Aruba controller for secure connectivity, no additional hardware is required. Software and configuration updates can also be accomplished automatically without any user intervention.

In addition to its remote access capabilities, VIA supports Suite-B cryptography for accessing government grade unclassified, confidential and classified information. When utilized within government networks, the VIA client works in conjunction with the ArubaOS Advanced Cryptography (ACR) module, which provides a securely authenticated and encrypted tunnel between the client and Aruba controller using NSA approved Suite-B algorithms.

The Aruba VIA client is currently supported on Windows, Mac, LINUX and iOS devices. Suite B capabilities are supported on all platforms.

REMOTE NETWORKING SOLUTION

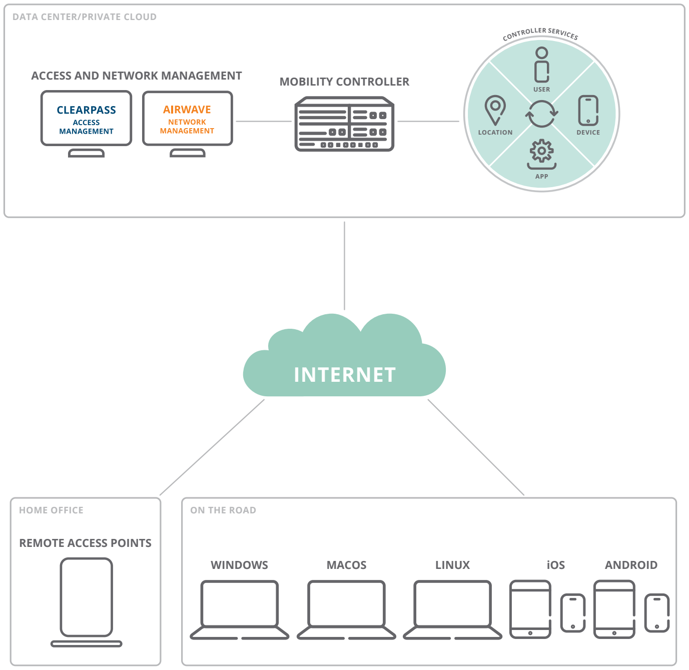


figure 11.0_100416_government-sga

Figure 11: Virtual Internet Access Client

Aruba Mobility-Defined Networks for Government

Government agencies recognize the need and productivity gains for deploying commercial, consumer-grade mobile devices, such as smartphones, tablets, and laptops. Doing so requires an architecture that supports users and their mobile devices in both an onsite WLAN facility and remote/global field areas where 3G and 4G capabilities exist.

The next generation of access networks must focus squarely on users and their devices, applications and locations. Aruba Mobility-Defined Networks are based on a user-centric, role-based access architecture, supporting secure mobility for wired, wireless and remote access. The components previously listed in this section are all part of Aruba Mobility-Defined Networks for Government. This architecture securely unifies disparate computing infrastructures, such as wireless, wired, and remote access VPN services, into one seamless network access solution – for government employees, contractors, visitors, and military personnel in garrison or in deployment. Authorized users are able to access network resources wherever they need them, with automatic access policy enforcement based on who they are – no matter where they are, what devices they use or how they connect.

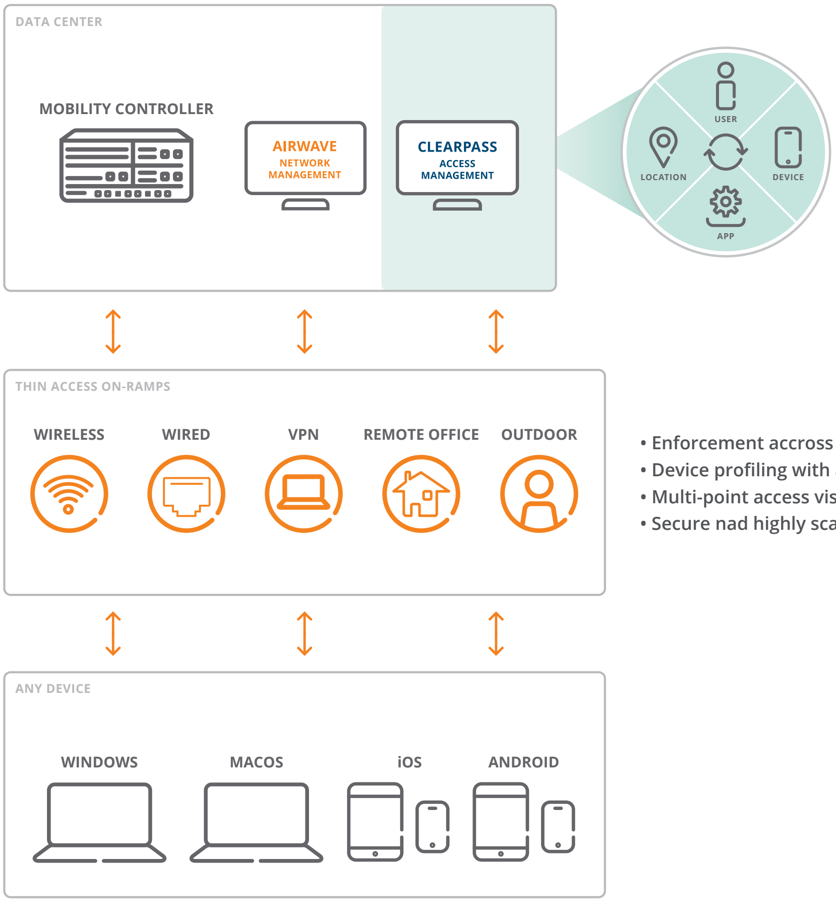
The Aruba Mobility-Defined Networks for Government architecture addresses the needs of the mobile enterprise by providing context-aware services that collects the following attributes for each session:

- User identity and role, such as government employee, contractor, visitor, etc.
- Device identity, including type, such as laptop, tablet, smartphone, etc.
- Application fingerprinting, including type (data, voice, video)
- User location (base, post, garrison, remote facility, etc.), time of day and access medium (wired, wireless, cellular)

This context-aware approach to network access eliminates the need to maintain VLANs at the network edge. Context-aware access policies allow IT to control users and devices so that employees can switch effortlessly between desktops, laptops, tablets, smartphones, and other mobile devices and have a single, consistent way to access the appropriate network resources.

Aruba Mobility-Defined Networks for Government provide a common set of network services that manage security, policy, and network performance for every user and device on the network, regardless of method of access. These services include:

- Identity management
- Device profiling and configuration
- Device posture check
- Context-based policy enforcement
- Application traffic management
- Guest access
- Content security
- RF Spectrum management
- Network configuration
- Compliance enforcement and reporting



- Enforcement accross any network type
- Device profiling with advanced posture
- Multi-point access visibility
- Secure nad highly scalable

figure 12.0_100416_government-sga

Figure 12: Expanded Mobility-Defined Networks for Government Architecture

Aruba Mobility-Defined Networks for Government support a wide range of network access modes that leverage its common set of network services to deliver consistent, reliable and secure context-aware access for users. These on-ramp access modes include:

- **Wireless Access Points:** Aruba 802.11n/ac APs support distributed and centralized traffic forwarding modes, while providing best-in-class RF management through Adaptive Radio Management (ARM) technology. All Aruba APs offer RF management and monitoring capabilities without requiring dedicated modes of operation.
- **Aruba Switches:** Aruba has extended the user-centric, services-based approach of the Mobility-Define Networks to a new class of wired APs. Designed to provide network access in wiring closets, Aruba switches with HPE Smart Rate connect wired Ethernet devices such as virtual desktops, IP phones, videophones, video surveillance cameras and 802.11 APs.
- **Remote APs:** Aruba Remote APs (RAPs) automatically extend enterprise resources to branch and home office networks using site-to-site VPN tunnels to the central data center. Using zero-touch configuration, employees at branch and home offices can easily set up their own RAPs with no IT assistance.
- **Outdoor:** Aruba outdoor rated access points provide dual-radio, multi-frequency capabilities to provide high-performance wireless mesh capabilities to outdoor environments.
- **Virtual Intranet Access (VIA) client:** This Aruba software client provides secure remote network connectivity for Apple iOS, Android, Mac OS X and Windows mobile devices and laptops.

Aruba Mobility-Defined Networks for Government combine advanced WLAN technology with government validated and policy compliant mobile device software supporting stringent government security regulations such as Common Criteria Certification, FIPS 140-2 Validation, DoD directives 8100.2 and 8420.1 Compliance. The solution provides this policy compliant and validated technology that all US government agencies are required to utilize.

Concept of Operations

Building an Aruba access network requires the key components described previously – Access Points (APs), centralized Mobility Controllers and optional ArubaOS software modules. These components can be installed and configured to support a wide range of environments and applications, such as building WLANs, large campus WLANs, outdoor mesh networks, and remote access solutions. A more detailed description of these use cases and deployment models can be found in a later section of this document.

The Figure 13 illustrates a typical Campus WLAN network topology with Aruba APs and controllers.

1. In this system, the centralized conductor and local mobility controllers are deployed in a combination of data center locations and communications closets/IDFs/MDFs. Conductor and local controllers should be selected and purchased based on their installation location and the size of network they will support, measured by both expected AP-count and user-count. If more network and controller capacity is required, additional local controllers can be easily installed and a portion of the existing network can be managed by the new controller.

2. The APs act as network-attached radios that perform only transceiver and air monitoring functions, commonly referred to as “thin” APs. APs should be selected based on the number and types of client devices to be supported, the availability of relatively clear 802.11 RF frequencies in the building(s) and the desire to “future proof” the network. For example, many organizations are now deploying high-throughput, dual-radio 802.11n/ac APs, configuring the 2.4Ghz radio to support legacy b/g client devices while simultaneously configuring the 5Ghz radio for high-performance 802.11n/ac client device connectivity.

   For more information on both controller selection and AP selection specific to campus network deployments, see the Aruba Campus Validated Reference Design Guide, found on Aruba’s website.

3. APs are installed according to a basic site plan that takes into account coverage and performance requirements, access point type, building construction and code requirements, Ethernet cabling availability (unless using mesh) and aesthetics.

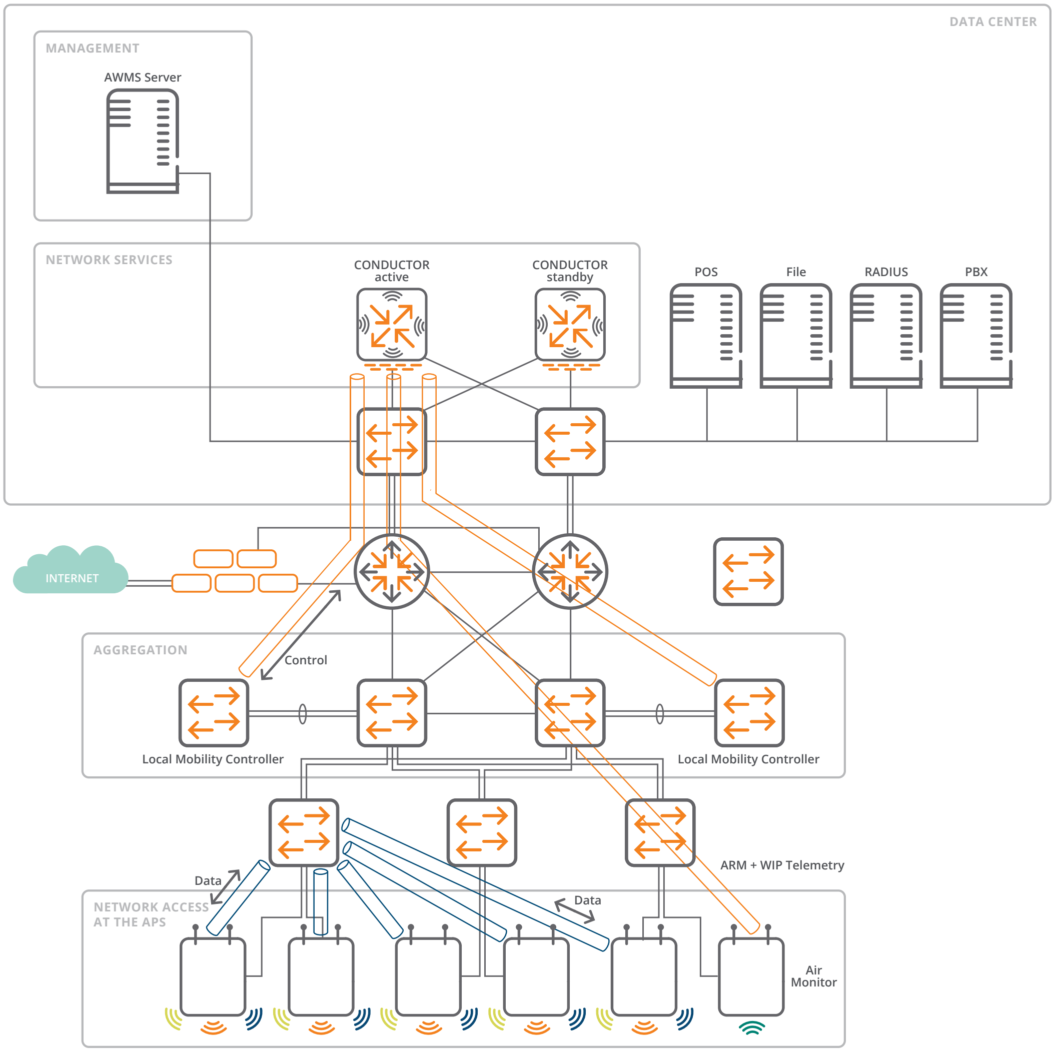


figure 13.0_100416_government-sga

Figure 13: Aruba Campus Wireless LAN Architecture

4. ArubaOS can be configured and monitored from the conductor controllers and/or the AirWave Management System – both have the capability of centrally managing the entire network of controllers and APs. The base network configuration (IP addressing, VLANs, 802.1X or other authentication methods, etc.) are configured and the optional software modules are activated through license keys and then configured for their operations. Policies, templates and AP grouping make the configuration management process both straightforward and also powerful in its flexibility.

5. Once installed and configured, the APs will be automatically and dynamically configured by their controller to meet the coverage and performance requirements according to the plan. This automated configuration method eliminates the complex site survey process required by earlier generation WLAN architectures.

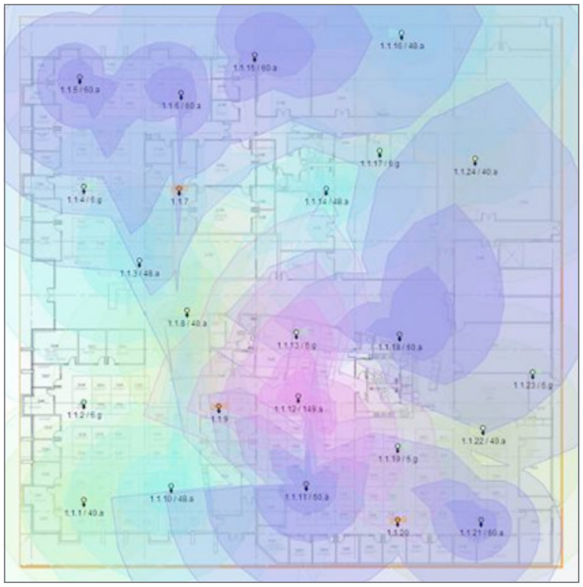


Figure 14: Example WLAN – AP Coverage Map

Aruba customers have heterogeneous networks, built on a wide variety of equipment, topologies, protocols and interfaces. Aruba products are designed for flexible, non-disruptive deployment in such environments. Because an Aruba network is designed as an overlay solution, the existing network is used only for transport – the wired network has no awareness that it is carrying wireless traffic. Therefore, the existing network need not be reconfigured or restructured in any way to add mobility. As long as there is an open IP communications path between the access points and their controller, the system will be 100% functional. This overlay WLAN architecture allows for a modular, phased introduction of mobility from pilot network to full-scale installation, deploying on top of existing L2 and L3 LAN/WAN infrastructure.

Further, the ability of the Aruba architecture to intelligently understand the data flows traversing the network has the end result of not requiring the deployment of separate VLANs to provide different network services. Aruba's unique architecture allows deployment of data, voice, and video services on the same VLANs, without negatively impacting the user community or security.

Client connectivity and traffic engineering and management within the Aruba architecture are very different than in traditional L1/L2 networks. Within a typically configured Aruba enterprise network:

1. Clients and users are authenticated prior to joining any production network or VLAN via standard Wi-Fi and AAA mechanisms.
2. All traffic is encrypted from the client, flowing across all L1/L2/L3 boundaries untouched (except by QoS mechanisms on outer headers), then arriving at the controller. In this manner, client-to-core security is provided where every traffic flow and packet is both authentic and eavesdrop protected.
3. The controller decrypts the traffic, intrinsically validating its source user.
4. The controller then passes the user's traffic through a series of traffic engineering rules and application-layer gateways for both performance management and security management purposes.

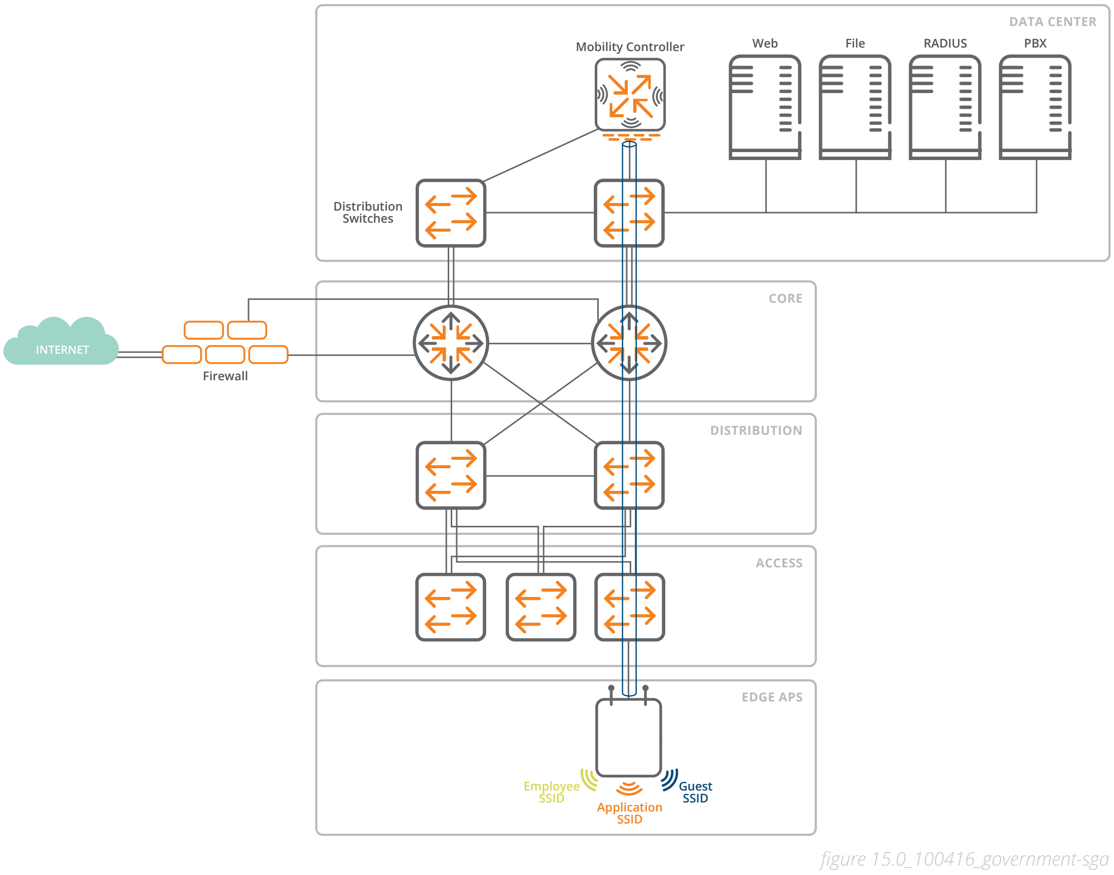


figure 15.0_100416_government-sga

Figure 15: Client-to-Core Traffic Encryption and Tunneling

5. In this architecture, the controller knows the state of the entire network, knows the state of all the users, and knows the state of all application traffic flowing across this part of the network. Many network engineering challenges simply evaporate and user requirements can be instantly met, such as:
    - Seamless roaming around the network, between floors and building and even IP-network domains
    - The need to ensure that all applications have their relative traffic priority levels adequately supported
    - The need to ensure QoS for voice activity emanating from the same device as data traffic, without complex VLAN/SSID designs
    - The ability to prevent peer-to-peer traffic between users on the same VLAN
    - The ability to tune broadcast/multicast traffic to ensure optimum handheld device battery life
    - The ability to enforce once complex security policies (e.g. limit peer-to-peer traffic) with now simple means (a central device for classification and enforcement)

These same components and feature sets are present in remote access solutions as well. With remote access solutions, controllers are typically deployed within a DMZ providing a public facing Internet interface. APs that are deployed in a campus environment can also be provisioned as Remote Access Points (RAP) to establish a secure IPSec connection to the controller. These APs are can be utilized in locations such as user residences, hotels or small branch facilities. The RAPs authenticate to the controller prior to actually becoming wireless access points. Once in access point mode, clients can then associate and authenticate to the network the same way they do in a campus environment. In essence, the campus network is extended to remote locations, allowing users and mobile devices to connect securely to the network. Once connected the same processes described above are in place, all transparent to the user.

To take remote access a step further, mobile devices with Wi-Fi and cellular 3G/4G capabilities, such as tablets and smartphones, can access enterprise network resources in hotspot areas or on the road through the use of Aruba's Virtual Intranet Access (VIA) client. This client can be installed from the controller onto the mobile device. Once installed, the user provides appropriate authentication credentials that will allow for a configuration profile to be downloaded to the client. The VIA client then establishes a secure IPSec or SSL connection to the controller on an as needed basis to provide the user access to enterprise network applications and resources. The same user roles and policies that are applied to users and devices in an enterprise and remote environment using RAPs can apply with the use of the VIA client as well.

Aruba's overall secure mobile solutions allows users and mobile devices access to the network from virtually anywhere, allowing for users to move and the network to follow them wherever they go.

DEPLOYMENT LOCATIONS AND TOPOLOGIES

The flexibility of the Aruba architecture lends itself to deployment in a variety of locations and topologies. This section explores how access networks for a wide range of government work environments can be built using Aruba components.

High-performance Indoor and Campus WLAN

Organizations have shifted from desktop computing to mobile computing such as laptops, smartphones and tablet PCs. Building a high-performance 802.11n/ac indoor and campus mobility network to carry both voice and data traffic is the most common deployment use case for Aruba.

This use case features a simple design, with an Aruba controller or controllers deployed in the network core or in a secure data center facility, with 802.11n/ac wireless APs installed at the network edge, placed throughout the campus as appropriate to provide the needed RF coverage and capacity. Buildings that are remote or have limited infrastructure can be linked to the existing core infrastructure via a mesh link, activated within the software on any Aruba AP. Users with laptops, tablets, handhelds, wireless phones and specialized devices can gain mobile access to networked applications, and are able to securely and seamlessly roam throughout the building and campus WLAN.

Below is a basic set of guidelines for designing an indoor/campus WLAN:

- Conductor controllers (the top-level controller in the hierarchy) are deployed in the network core or in a secure data center. Management of this network takes place on the conductor controller and/or the Aruba Airwave management platform.
- The controllers are configured to utilize one or more RADIUS or PKI servers (Microsoft, Juniper, Cisco, etc.) for user authentication.
- The controllers perform network access control functions during the user login process and traffic engineering functions during user-traffic flow.

- Local controllers (optional depending on network scale and geography-topology) can be deployed in either the data center or in the network access, distribution or core layers of the network.
- Conductor controllers and local controllers can be separated by large geographic distances. Also, one pair of conductor controllers can service many local controllers at many distributed site locations.
- Indoor 802.11n/ac access points with integrated antennas (typically) are deployed in the user space according to an appropriate RF plan, with an AP deployment density based on application, coverage, performance and capacity requirements.
- Where possible, capable 802.11n/ac clients should be supported using a 5Ghz channel plan and 802.11 b/g clients should be supported using a 2.4Ghz plan. This will ensure maximum performance and capacity for the 802.11n/ac clients while simultaneously preserving support for legacy devices.
- APs are typically powered by Ethernet PoE switches, but can also use AC adapters or PoE injectors.
- The L2/L3 network configuration between the APs and controllers are immaterial – configurations can be created on the conductor controller to accommodate almost any L2/L3 network design.
- A configuration is created and activated on the conductor controllers that defines:
  - L2 and L3 integration
  - RF and AP configuration
  - FIPS-encryption configuration and policies
  - User, security and access policies
  - QoS and traffic management policies
- All APs are automatically and dynamically managed by the controller and go active, allowing authorized users to securely connect through the APs and controller to the backbone network.

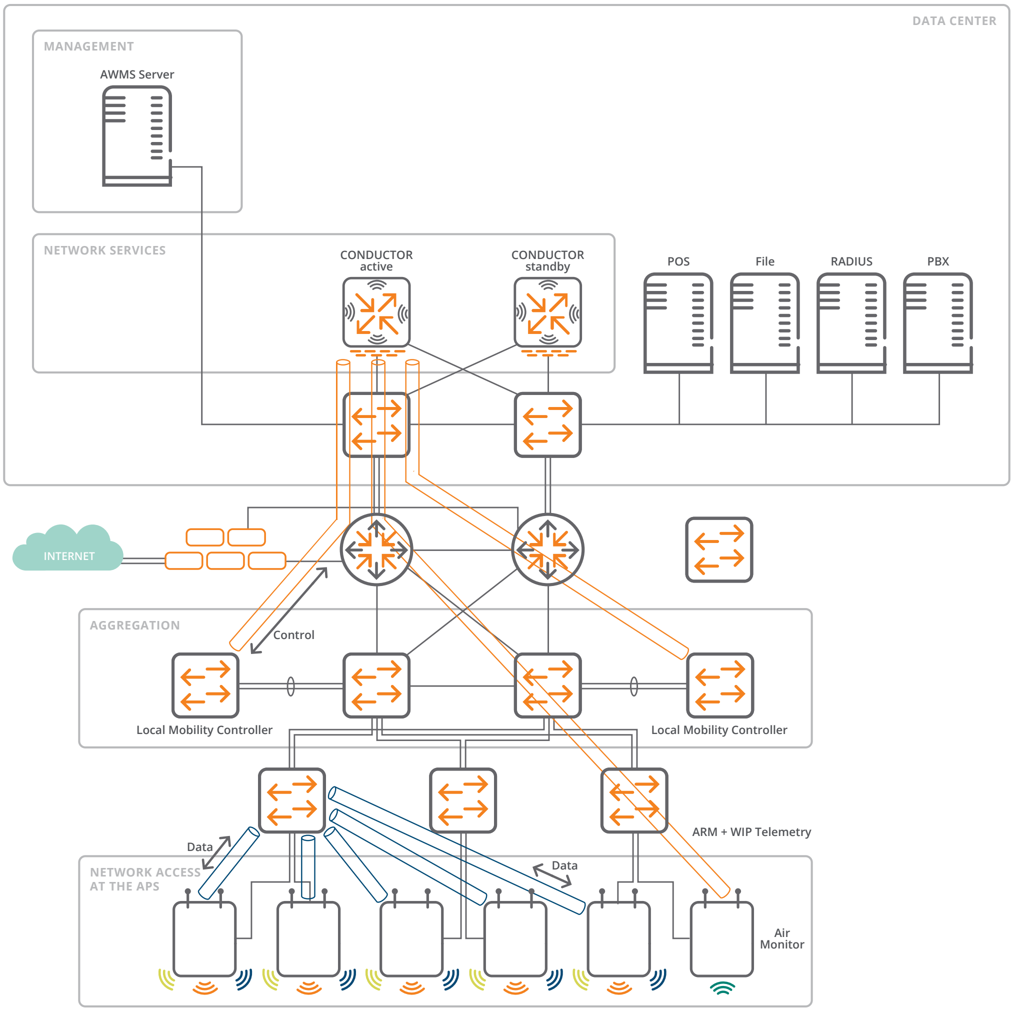


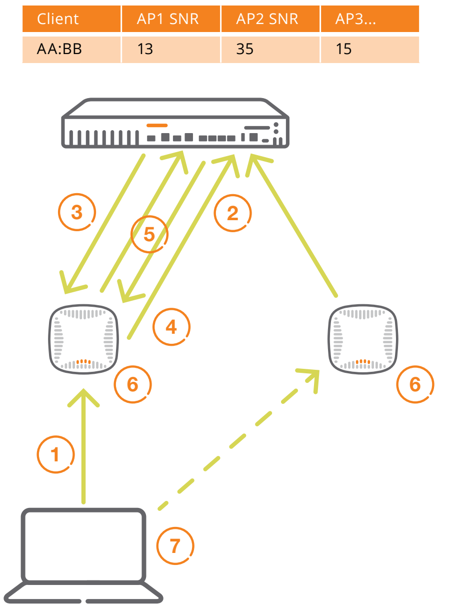
figure 16.0_100416_government-sga

Figure 16: Aruba Campus Wireless LAN Architecture

More detailed information on this network design can be found on the Aruba website in the document Campus Wireless Networks Design.

The characteristics and benefits of the Aruba architecture in the high-performance WLAN use case are:

- **High Performance:** Aruba's 802.11n/ac Wave 2 APs are designed for 1,733 Mbps peak throughput in the 5-GHz band and 800 Mbps in the 2.4-GHz band. Additional network and user capacity can be added to the network at any location by simply adding APs to the area, which will automatically be configured and utilized by the system.
- **Aruba ClientMatch™:** On Aruba 802.11ac wireless access points, ClientMatch eliminates sticky clients by continuously gathering session performance metrics from mobile devices and steering clients to APs with a better connection. ClientMatch dynamically optimizes Wi-Fi client performance, even while users roam and RF conditions change. If a mobile device moves out of range of an AP or RF interference impedes performance, ClientMatch steers it to a better AP to maximize Wi-Fi performance. The result is higher throughput and better overall performance for all devices connected to the WLAN.
- **Reduced Reliance on Wired Networks:** The wired-like performance of Aruba's 802.11n/ac wireless LAN presents an option to reduce the reliance on edge Ethernet switches, as users migrate away from fixed desktops to Wi-Fi-capable devices. Especially useful during an edge switch refresh, offsetting wired port costs with cost-effective 802.11n/ac wireless LANs can significantly reduce equipment upgrade bills. The result is a network that enables user mobility, while lowering energy usage and annual maintenance costs.
- **Self-configuring:** Aruba's Adaptive Radio Management (ARM) delivers reliable self-optimizing wireless performance with features such as Band Steering, Co-channel Interference Mitigation, Adjacent Channel Noise Mitigation, Spectrum Load Balancing and Air-Time Fairness. ARM technology ensures that the wireless network is always optimized for local conditions and will automatically adjust power, channel, band, access point loading and other parameters to ensure reliable high-speed operation, even in extremely crowded and challenging environments.



Client	AP1 SNR	AP2 SNR	AP3...
AA:BB	13	35	15

CLIENT MATCH: HOW IT WORKS

1. Client connects to a radio
2. All radios reports probe request that they hear from the client back to the controller
3. The controller builds VBR a client centric view of the network and shares it with the associated AP The AP now has visibility into all of the available radios for the client. The AP determines if the client is connected to the optimum radio based on:

   Signal Strength
   Channel Utilization
   Band
4. AP notifies controller if there is a better radio for the client
5. Controller coordinates steering across APs
6. Client is moved to the optimum radio

Decision information is logged on the controller and sent to AirWave

Step 2 will be replaced by the 11k beacon reports when available from the client

Step 6 will leverage the 11v QBSS transition element when available

Steps 2-6 are repeated as long as the client is on the network

figure 17.0_100416_government-sga

Figure 17: Aruba ClientMatch

- **Application Visibility:** Aruba's AppRF technology is an important tool for controlling what applications can be used and how much bandwidth they are allowed to consume on the network. In addition to classifying the web sites by content category – gambling, pornography, news, etc., websites are rated by their "reputation". This is a measure of how likely an end user may be infected, or become the victim of a phishing scam, or some other threat. The score is affected by presence of malware on the site, links to other questionable sites, how long the web site has existed, how long it has been since it was last infected and other similar statistics.

  AppRF Dashboard provides:

  - Web browsing breakdown by categories and risks
  - The ability to use web categories and risks in AppRF policy making
  - Blocking of, QoS, Bandwidth limit, mirror, log web content
  - "Security" web category allows blocking of sites that present a security risk to end users
  - Full AMON logging of web site information into AirWave
  - Simple web notification to users who violate policy

- **Skype for Business Solution:** In both wired and wireless environments, Aruba offers a full Skype for Business solution that prioritizes Skype network traffic and enhances the user experience. That means fewer dropped calls and a higher quality video. In a wireless environment, Aruba leverages SDN integration with Microsoft Skype for Business and AppRF technology to ensure a predictable unified communications experience. And only Aruba offers end-to-end diagnostic visibility correlated across the Skype server and mobility network, which simplifies operations for the network and telecom staff.

  Over the wired access layer, the HPE Network Optimizer SDN Application for Skype for Business enables automated provisioning of network policy and quality of service to provide an enhanced user experience for Skype for Business sessions. The HPE Network Optimizer SDN Application dynamically provisions the end-to-end network path and applies QoS policy via the HPE Virtual Application Networks (VAN) SDN Controller, reducing the need for manual, device-by-device configuration, which greatly simplifies policy deployment and reduces the likelihood of human errors.

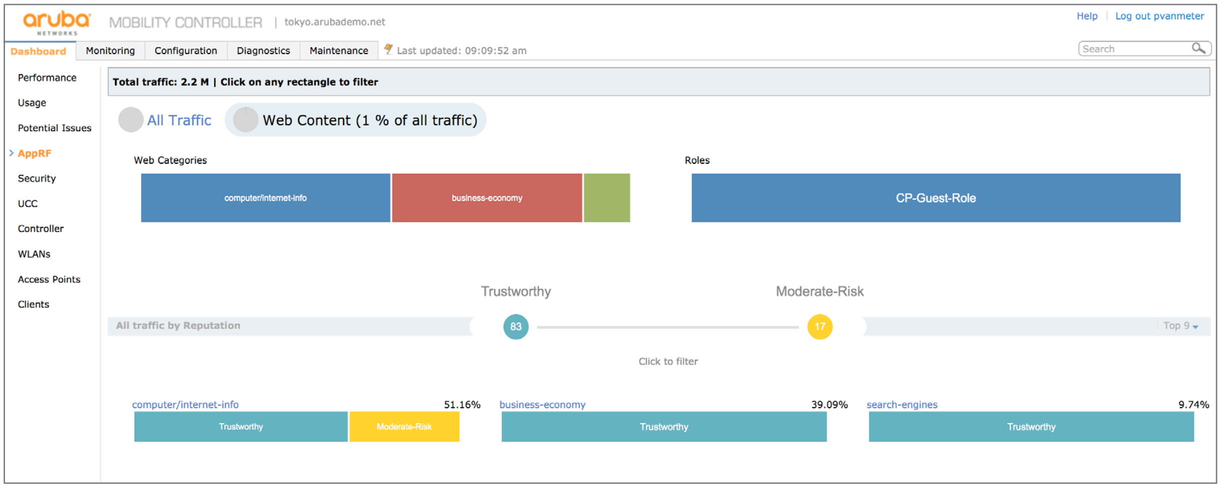


Figure 18: AppRF and Web Content Classification Dashboard

- **Government-grade Security:** Aruba's controllers provide a Common Criteria validated policy enforcement firewall, client-to-core encryption, user authentication, and a host of other security features to ensure privacy and protects network integrity for all users. Rogue detection and WIPS can identify client and access point attacks and, in many instances, prevent them from occurring.

Warehouse, Industrial, Outdoor and Mesh WLAN

For industrial and field environments, secure WLAN access networks increase productivity by bringing the access network to personnel instead of forcing them to go to fixed workstations. By simultaneously supporting data, voice and streaming video, wireless networks provide full access to existing applications and enable new ones such as all-wireless mesh-based telemetry, voice recognition and streaming video surveillance. Wireless networks reduce the need for expensive network-related power and data cable plant and equipment, lowering capital expenditures and mitigating potentially expensive maintenance headaches.

Wireless mesh networking makes it easy to extend IP connectivity where no cabling plant exists, and is most commonly used to take wireless networks outdoors – enabling a host of applications to previously underserved areas. In the government sector, there are numerous situations that can be addressed by wireless mesh including continuous connectivity for large areas such as military bases, forts and camps, hospital grounds, education campuses, warehouses, surveillance coverage for fence lines and communications for security forces.

Wireless access in outdoor environments presents their own set of unique issues and requires solutions that deal with both natural and man-made obstacles, as weather and topology present challenges to the reliable operation of wireless networks and their equipment.

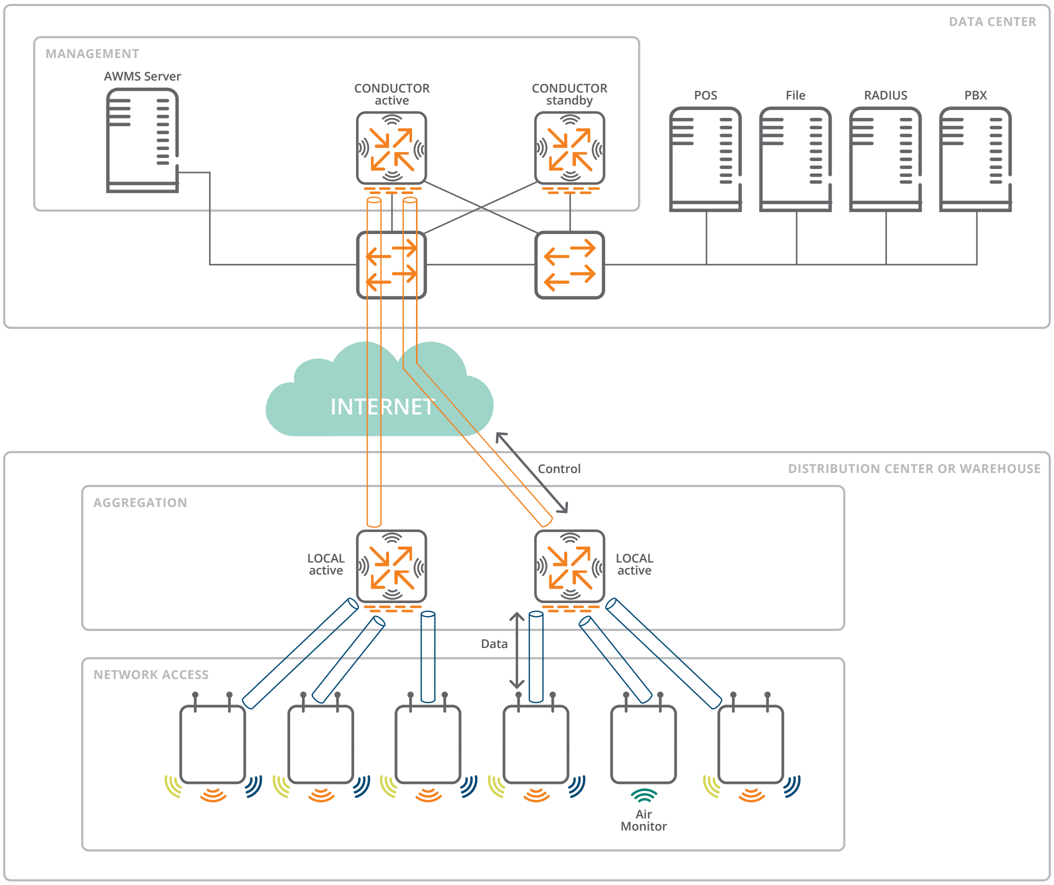


figure 19.0_100416_government-sga

Figure 19: Warehouse/Distribution Center Logical Design

Below is a basic set of guidelines for designing an outdoor/ mesh WLAN:

- Similar to an indoor or campus WLAN design, outdoor and industrial WLAN designs involve controllers that are installed in secure communications facilities and APs installed in areas that require wireless access coverage.
- Deployed APs are either outdoor-rated (such as Aruba's AP-275) or indoor APs installed in the proper type of enclosure with external antenna connectors.
- APs may be connected by Ethernet (fiber or copper) or by activating the Mesh feature found within ArubaOS that provides AP-radio to AP-radio backhaul connectivity.
- Antenna selection and installation is based on the physical environment and the desired coverage pattern, and may include:
  - Omnidirectional antennas for client access coverage, including more specialized down-tilt antennas
  - Directional antennas with narrow beam width to provide a point-to-point connection to another AP using the Mesh feature capability found within ArubaOS
  - Directional antennas with wide beam width to provide partial coverage to an intended access area or to provide a multipoint mesh connection
- AP power may be provided by a number of different power options – including solar panels, battery, low-voltage DC power, high voltage AC and Power-over-Ethernet.
- The network may only require a single SSID if the Aruba controller is used to appropriately perform security and QoS traffic management functions based on the identified user, device type, location and application.
- Special consideration should be given to ensure support for all applications, including data acquisition and control systems, specialized handheld devices/applications and voice over WLAN. The wireless network will require continuous real-time optimization to reliably support mobile voice, bar code scanning, inventory management and data terminal applications in the presence of noise and interference. Using standards-based mechanisms such as 802.1p and DSCP QoS tags, Aruba networks monitor the type and traffic patterns of applications in use and automatically adjust parameters to ensure reliable application delivery.

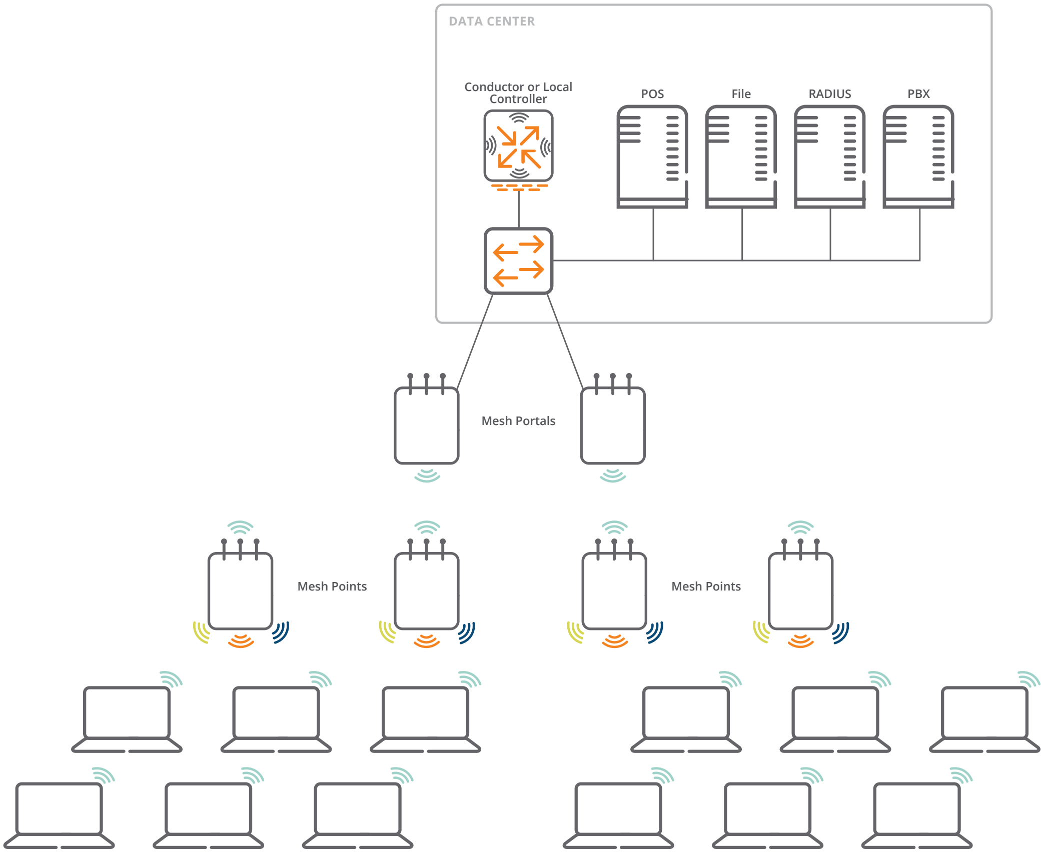


figure 20.0_100416_government-sga

Figure 20: Example Mesh Configuration

- The Mesh feature set is used to provide intra-network backbone connectivity between APs when no Ethernet or alternative backhaul is available at the AP installation location.
  - Client access APs (called Mesh Points) are single or dual radio APs that provide access to the local client devices
  - Aggregated client traffic is carried across one or more mesh hops to one or more Ethernet connected APs (called Mesh Portals)
  - By employing centralized cryptography on the controller instead of "per hop" encryption, no performance penalty nor security concerns arise
- Similarly, special consideration should be given to interoperability security requirements for low power, battery operated handheld devices potentially sourced from multiple vendors. Mobile applications run on a wide-variety of application-specific devices (ASDs) that differ in form, input and output capabilities, operating system, security capabilities, radio types and more. The use-case differences present a special set of "mobility performance" requirements on the mobility infrastructure such as fast roaming, load-balancing and battery life improvements. To support and secure a heterogeneous set of mobile device types, Aruba's architecture boasts a device agnostic approach. The Aruba solution follows an open standards approach and therefore does not require any proprietary client-side hook-ins or client side software for full interoperability and "mobility performance".
- Consideration should be given to the design for simple coverage versus high performance, where the former design goal will require fewer installed APs but will limit overall guaranteed throughput depending on client location.
- In an outdoor environment, consideration must always be given to the topography and changing environmental characteristics to ensure the design meets performance criteria even in the worst possible RF conditions.

For more information, please browse the Aruba website to access the Outdoor Mesh Solutions Guide.

Secure Remote Access

Aruba offers a new approach for remote networking that eliminates the cost and complexity barriers of deploying secure remote network services for government agencies. The Aruba solution allows customers to extend the data center footprint wherever users need it, through low-cost access devices and low-cost commodity network transport. The following provides an overview of the Aruba Virtual Branch Network (VBN) solution and its key features and components.

Branch offices, satellite clinics, teleworkers, temporary workers, and traveling military commanders all require access to mission-critical data from the agency or service data center. Traditional remote networking solutions designed to address this need have either relied on virtual private network (VPN) clients or replicating routing, switching, firewall and other services at each remote location. Client VPN solutions address only a single device and require revision control and driver compatibility management and may not be available for all platforms. Additionally, the remote user experience differs from that of a campus user, necessitating end user training and often resulting in help desk calls. In cases in which IT has to replicate a network infrastructure at every remote location, costs are high and deployment/maintenance is complex.

Aruba's VBN solution dramatically simplifies the complexity and cost of deploying a remote access solution at a branch or teleworker site. Complex configuration, management, software updates, authentication, security and remote site termination tasks are handled by powerful data center-based Aruba controllers running FIPS certified ArubaOS software. Network access and management services are virtualized in the data center controllers and then pushed to low-cost, purpose-built remote access points (RAPs). RAPs provide secure connectivity and deliver centralized services to end users. FIPS certified Layer 3 IPsec tunneling between the controllers and RAPs allows any wide area network – including 3G cellular, hotel guest connections and broadband internet – to be employed.

The VBN solution differs from traditional remote access solutions by focusing on user policy – instead of ports, routing, subnets and VLANs. Aruba's distributed policy enforcement firewall delivers policy-based control, enhanced security, and support for differentiated services based on user-type/role and is always under IT control. The VBN solution is persistent, easily configured, requires no user training and delivers a plug-and-play experience that results in a more uniform and secure user experience – regardless of user location. All policies are uniformly enforced, delivering the same user experience over both wired and wireless networks.

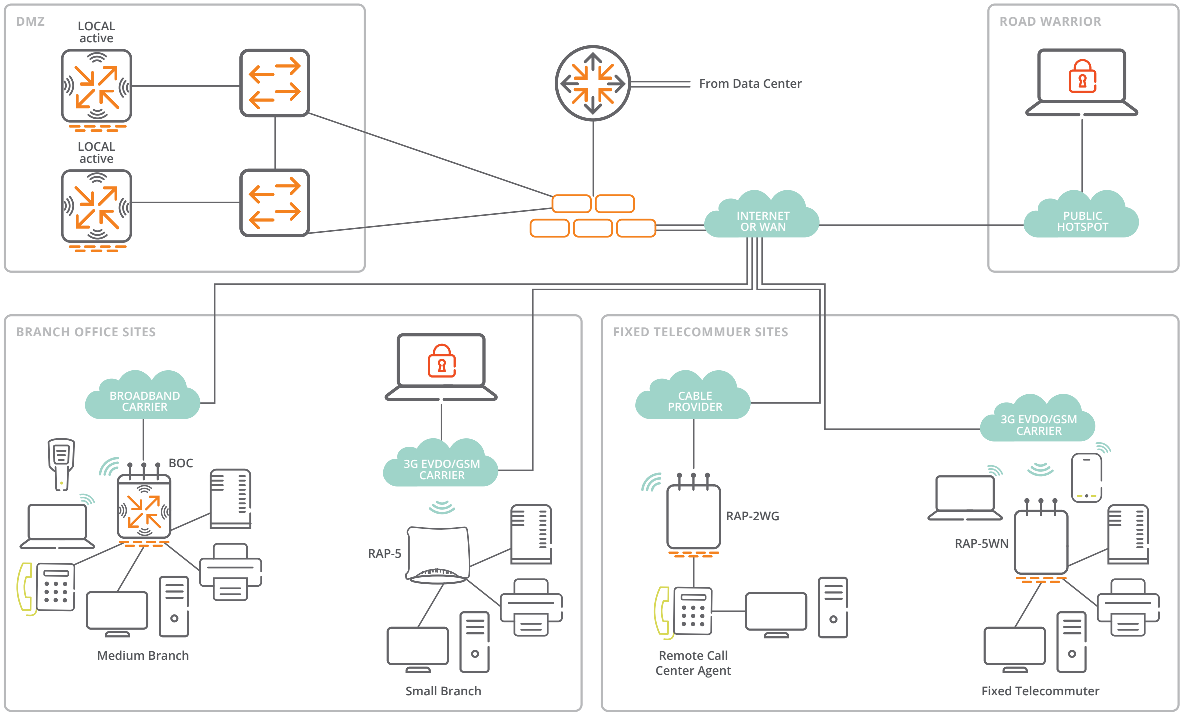


figure 21.0_100416_government-sga

Figure 21: Virtual Branch Network Logical Design

Below is a basic set of guidelines for designing a Remote Access network based on the Aruba VBN concept:

- Conductor controllers are logically deployed in a secure data center as shown on in the diagram below. All management of this network takes place from the conductor controller and/or the Aruba Airwave Management platform.
- The controllers utilize one or more RADIUS or PKI servers for device and user authentication.
- Access points (called Remote Access Points or RAPs) are deployed in remote locations. A remote location might be a Small Office/Home Office (SOHO) or a small branch office with multiple users and multiple devices. The RAP can be placed in a fixed location (e.g. an apartment, a house) or used portably.
- Any Aruba AP can be utilized as a RAP. The AP 320, 330 and 220 802.11ac series APs have an additional Ethernet port that allows the connection of wired devices, such as IP phones, laptops, etc., if desired. Crypto assist co-processors provide line-rate encryption of all wired network traffic.
- Any IP-backhaul can be used to provide connectivity from the RAP's WAN-facing Ethernet port across an "IP cloud" to the controller, including broadband Internet connections, hotel and office guest networks and SATCOM terminals. The Aruba RAP-155, 205H, and 100 series have the additional capability through its USB port to utilize wireless 3G or 4G connectivity to provide backhaul when a wired connection is not available or not desirable.
- The local network configuration and the IP network topology between the APs and the controllers is immaterial – as long as there is a valid IP connection with a minimum amount of bandwidth available (128Kb/s +) – the agency/service network and all logical SSIDs are extended seamlessly to the Remote Access location.
- Both wired devices (VoIP phone, desktop PC, printer, security camera) as well as wireless devices can be supported simultaneously.
- Additional "overlay networks" can be operated on top of this L2/L3 remotely extended network, including TYPE-1 cryptosystems for SIPRNET access.

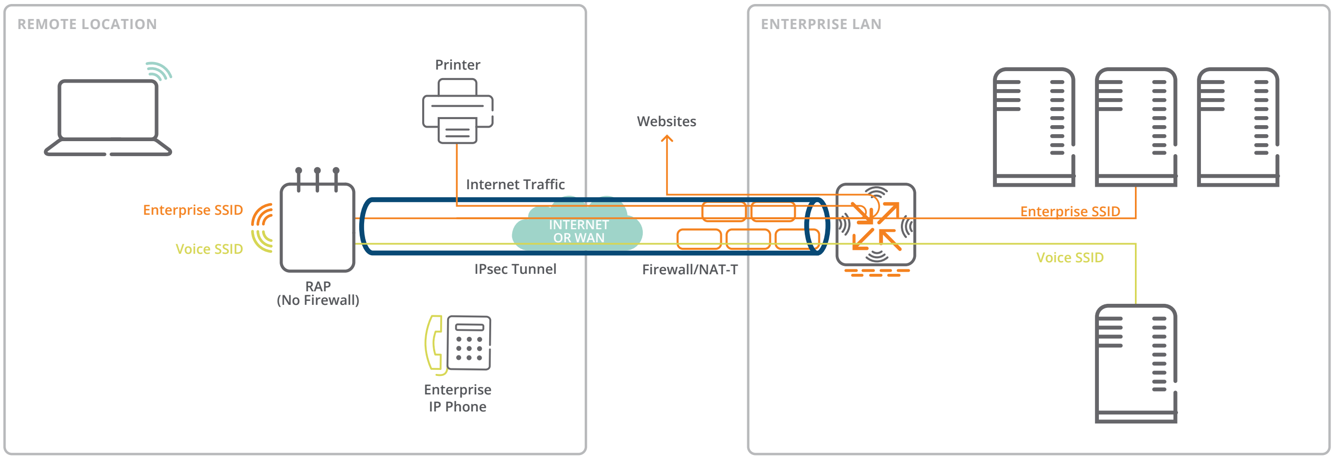


figure 22.0_100416_government-sga

Figure 22: Secure Connectivity from the Clients/AP to the Controller vai Any Backhaul

For more information on secure Remote Access network design, please browse the Aruba website to access the Aruba Remote Access Point (RAP) Networks Validated Reference Design.

Aruba's VBN solution is designed to eliminate the pain points that are common in traditional remote access solutions. Key benefits of this solution are:

- **Secure Communications – Across Any Backbone:** All network components of the solution benefit from government-grade, agency-validated security, including FIPS 140-2, DISA UC-APL, and Common Criteria validations. Any commodity transport, such as standard broadband can be used in lieu of costly private networks.
- **Centralized Security and User Access Control:** Centralized policies and user access control render secondary firewalls to protect the remote network unnecessary. Security is consistent across the entire solution for each user. The same authentication methods and encryption algorithms are utilized, no matter where the user accesses the network. The user's role follows them everywhere; the same access policies and rights are enforced and used regardless of the location of the user.
- **Simplicity:** The IT provisioning model seamlessly joins a remote access point to the enterprise network without additional log-on credentials or software to launch. Applications and devices securely join the logically extended network and work out-of-the-box without additional configuration. End-user access is simplified – the user connects, authenticates and accesses the network the same way everywhere, whether in their home, hotel room, remote branch office, automobile or anywhere else. No VPN clients or additional credentials are required for access – which results in fewer mistakes and removes the need for training the end user.
- **Support for Any Remote Device and Application:** Policy-based forwarding ensures that IP-based devices (tablets, smartphones, VoIP phones, laptops, etc.) and services work as well remotely as they do locally – without the need for separate voice networks and related security infrastructure. The security posture of these remote devices can be further enhanced by encrypting their traffic and policing it in the data center to ensure only the right ports, protocols and servers are used. All applications, whether data, voice or video, are accessed the same anywhere the user is located. The Aruba controller consolidates access management on a single platform.
- **Centralized Management:** All management and control functions are centralized in the Aruba controller. This user-centric management architecture eliminates the need for a separate management infrastructure and provides visibility to all users and devices, speeding fault isolation in the event of a problem. All software updates are performed by IT. These updates are automatically pushed to the RAPs without end-user intervention.

Deployable Networks

In some government agencies, the job location itself is variable as personnel are dispatched to where they are needed most. In these situations, the ability to access communication networks on a moment's notice is critical. Aruba's deployable wireless LANs are readily scaled from dozens to thousands of users and can enable the most mobile professionals – like first responders and military personnel – to easily and securely connect to off-site networks and applications. The robust design and simple operation of Aruba's WLANs and network security systems makes them well suited for rapid deployment scenarios – aiding public safety and Homeland Security missions such as national catastrophes and disaster relief, as well as military activities like training exercises and support of temporarily deployed command staff, personnel and teams.

Aruba's deployable solution provides hardened, secure WLAN systems that can be field deployed in varying configurations based on mission length, force structure and communications requirements. The Aruba wireless LAN is FIPS 140-2 compliant and provides instant-on, rapidly-deployable wireless access to both classified and unclassified networks. Small WLANs can be deployed with an Aruba multi-service controller and several outdoor or APs that provide connectivity for a few personnel during a brief deployment. Large WLANs can be created through the formation of a hierarchical topology involving a combination of multiple controllers and APs meshed together and classic "AP grid deployments".

RAPs can be deployed to support secure remote access for both wireless and wired connections. Some RAPs have multiple wired ports to support devices such as wired laptops, IP Phones, and VTC equipment. Inline Type-1 HAIPE encryptors can also be utilized for classified data access via SIPRNET. Additional information regarding integration with Type-1 HAIPE solutions is available later on in this guide.

A resilient, self-healing mesh, working in conjunction with Aruba's Adaptive Radio Management (ARM) technology, enables radio signals to reliably hop from AP to AP without the need for data cabling. ARM automatically compensates for interference, network traffic and even the types of applications that run on the network. As a result, data, voice, and video applications have sufficient network resources, including airtime, to operate properly.

Mesh operation allows wireless APs to be located and relocated anywhere, quickly and reliably in even the most hazardous conditions without installing data cabling or making site modifications. The elimination of an Ethernet backbone reduces complexity and setup time as well as increases network reliability through the avoidance of cable-displacement outages.

Aruba's client-to-core security includes embedded user access control, centralized encryption, a policy enforcement firewall and wireless intrusion detection. The firewall classifies traffic on the basis of user identity, device type, location, and time of day and provides differentiated access for different classes of users. Access is tightly controlled, and each user's application traffic is inspected and validated against security policies to ensure compartmentalization between user groups.

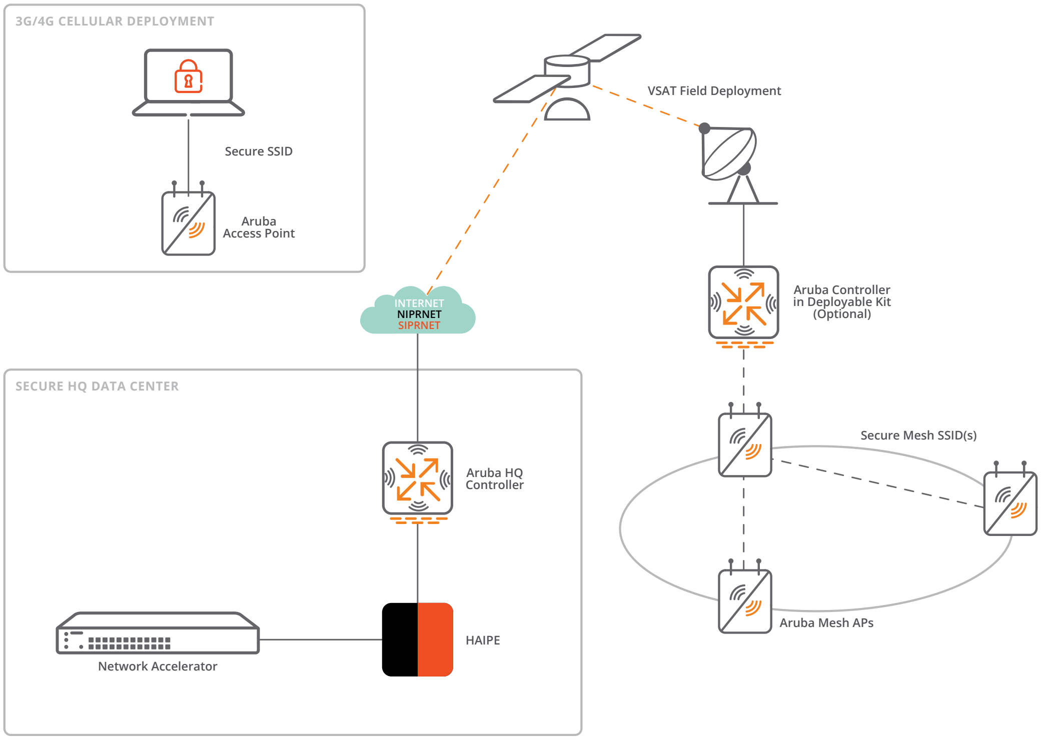


figure 23.0_100416_government-sga

Figure 23: Deployable Solution via RAP – 3G or SATCOM Backhaul

Key benefits of the Aruba deployable networks solution are:

- **Secure communications:** Government compliant, secure wireless LANs ensure all data is securely encrypted end-to-end, all the way from client to the Aruba controller housed in the HQ data center. Aruba is the first wireless LAN vendor to support stringent government security regulations such as Common Criteria and UC-APL certification, FIPS 140-2 Validation and DoD directive 8100.2 Compliance.
- **Ease of set up:** Aruba's WLANs can be set up or taken down within minutes with a single, centrally managed and secured remote AP and can be easily scaled from a few users to thousands. When using Aruba wireless mesh network features, APs can be deployed without the use of any intervening data cabling and can be installed, moved, or changed quickly. Custom AP packaging is available through key government integrators that provide an environmentally hardened, battery powered portable solution that allows local WLAN connectivity for many hours to days without a local power source.
- **Rapid, automatic local configuration:** Aruba's Adaptive Radio Management (ARM) software eliminates the need for site surveys prior to activation by using automatic, infrastructure-based controls to maximize client performance and enhance the stability and predictability of the entire Wi-Fi network, regardless of the local RF.
- **Real time application support:** The Aruba solution wirelessly transmits data, voice and video over one network that is uniquely configured for high latency/low speed links such as SATCOM and cellular. Aruba's ARM software allows mixed 802.11a/b/g/n/ac client types to interoperate at the highest performance levels, allocates RF airtime fairly and avoids or mitigates co-channel interference.
- **Centrally managed controllers:** Aruba controllers perform all of the complex tasks such as RF optimization and AP management and integrates all the components needed to deploy a secure WLAN solution – including an identity-based policy enforcement engine, Wireless IDS, Client integrity, Layer 2 encryption and remote access.

Virtual Mobility Controller for Tactical Deployments

DoD customers have a need for hardened, mobile, tactical MILSPEC solutions for battlefield mobility. The Virtual Mobility Controller (VMC) platform is secure ArubaOS software available in a small form factor suitable for DoD deployments. Deploying an x86 based virtual controller on certified MILSPEC platforms allows for greater flexibility in deployment options for customers. Supporting full-featured access allows for continuity of operations from the enterprise to the battlefield.

VMC Tactical Capabilities:

- IPSec VPN – QA Tested for IPSec Site-to-Site VPN supporting Suite-B Cryptography
- VIA – Windows, MacOS, IOS, Android, and Linux supported clients. Supports both AES and Suite-B IPSec from VIA clients
- AP and WLAN features
- VMC Tactical Certifications:
  - FIPS 140-2
  - Common Criteria
  - Listed on CSfC Components List

Example Tactical Platforms:

- PacStar 451
  - Intel Dual-Core i5, 16 GB RAM, 2 GE ports (CPU limits 1 VMC-TACT only)
  - Intel Quad-Core i7, 16 – 32 GB RAM, 2 GE ports
- DTECH TXC4
  - Intel Core i7, 8 – 16 GB RAM, 256 – 1 TB SSD, 1 – 4 GE ports
- Klas VoyagerVM
  - Intel Core i7, up to 16GB RAM, up to 4TB SSD
- Oceus MPSP
  - 1 Server Unit: Dual 8-Core 2.1 GHz Processor, 32 GB DRAM, 1024 GB SSD Licensed Virtualization SW (Optional)

VMC Tactical Use Cases

WLAN Capability Package

- Outer tunnel Layer 2 Secure Wi-Fi
  Aruba AP's terminate "outer" tunnel (WPA2) onto the Aruba VMC
- Inner tunnel Layer 3 IPsec VPN
  Other Vendor VPN Client and gateway supporting Suite-B algorithms

Site-to-Site VPN (Outer Or Inner Tunnel)

- Suite-B algorithms required for both peer ECDSA certificate authentication and AES-GCM encryption
- Aruba VMC can terminate to another VMC, 7000, or 7200 series controller dependent on deployment architecture
- Aruba controllers can be either Inner or Outer VPN component
- Vendor 2 VPN Gateways provide 2nd Suite-B IPsec tunnel

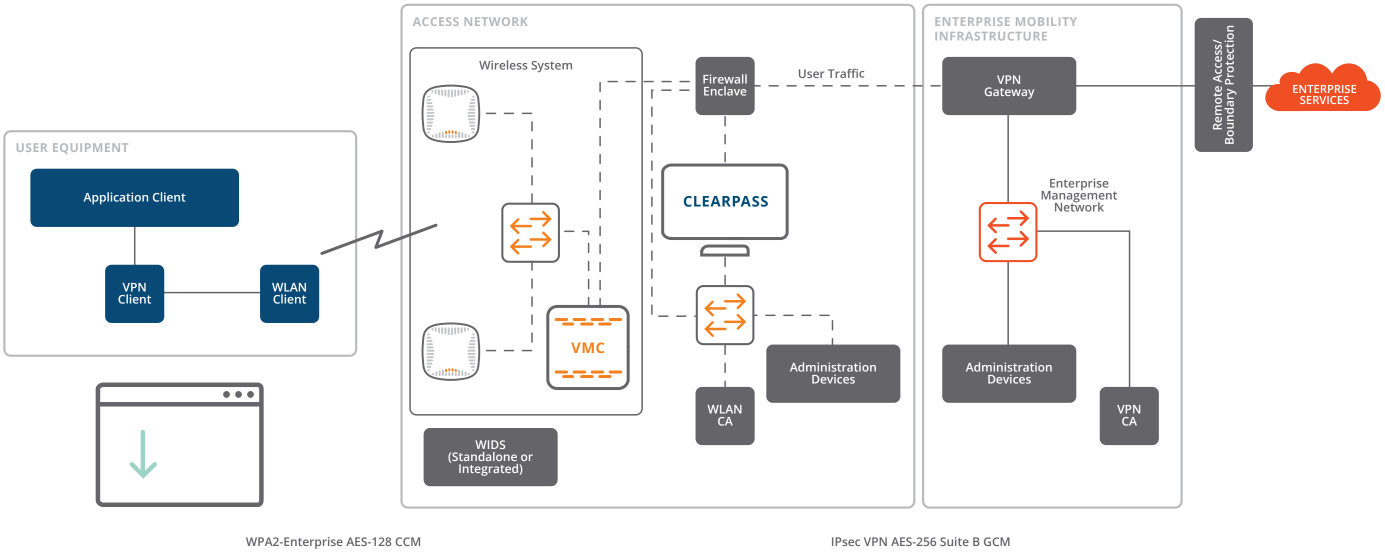


figure 24.0_100416_government-sga

Figure 24: WLAN Capability Package

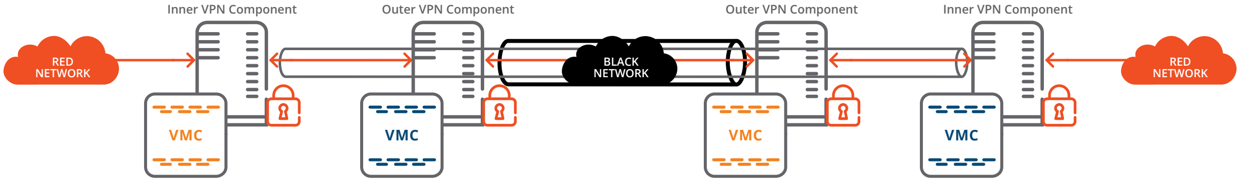


figure 25.0_100416_government-sga

Figure 25: Site-to-Site VPN (Outer to Inner Tunnel)

VPN Solution with End User Device

- Aruba VMC can be positioned as inner or outer tunnel termination gateway
- Virtual Machine on client needed when executing two Layer-3 Suite-B VPNs
- Aruba VIA Suite-B IPSec client on mobile device (on outer VM or inner VM) terminating the Aruba VMC
- Optional Layer 7 TLS v1.2 could serve as inner application tunnel

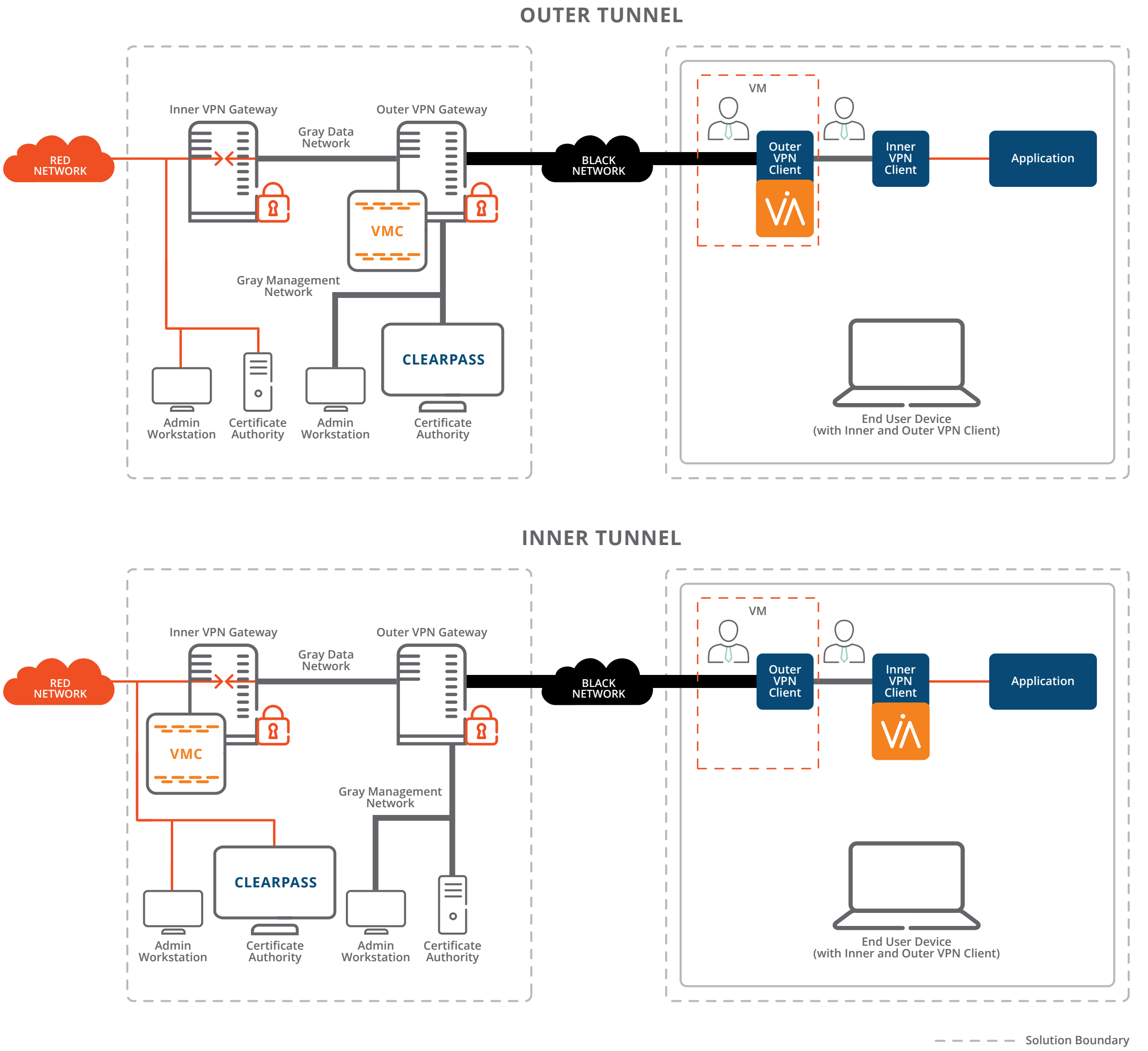


figure 26.0_100416_government-sga

Figure 26: VPN Solution with End User Device

Mobile Access over Private LTE

- Based on the Mobility Access Capability Package, but uses Suite-B based private LTE as the outer tunnel
- Aruba VIA Suite-B IPSec client installed on the mobile device as the inner tunnel, terminating on the VMC

Multiple Classification Site-to-Site

- Based on the Mobility Access Capability Package, but uses Suite-B based private LTE as the outer tunnel
- Aruba VIA Suite-B IPSec client installed on the mobile device as the inner tunnel, terminating on the VMC

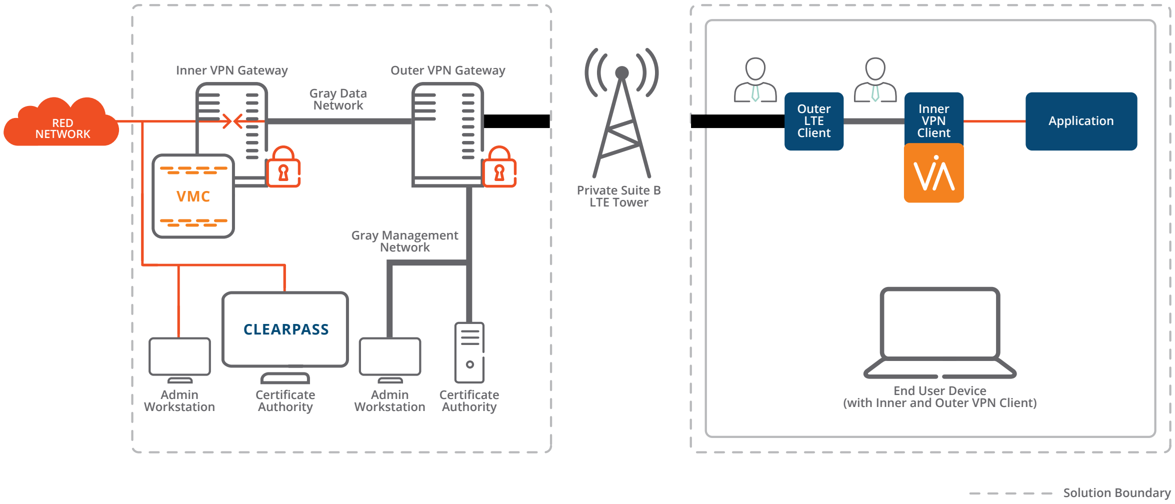


figure 27.0_100416_government-sga

Figure 27: Multiple Access over Private LTE

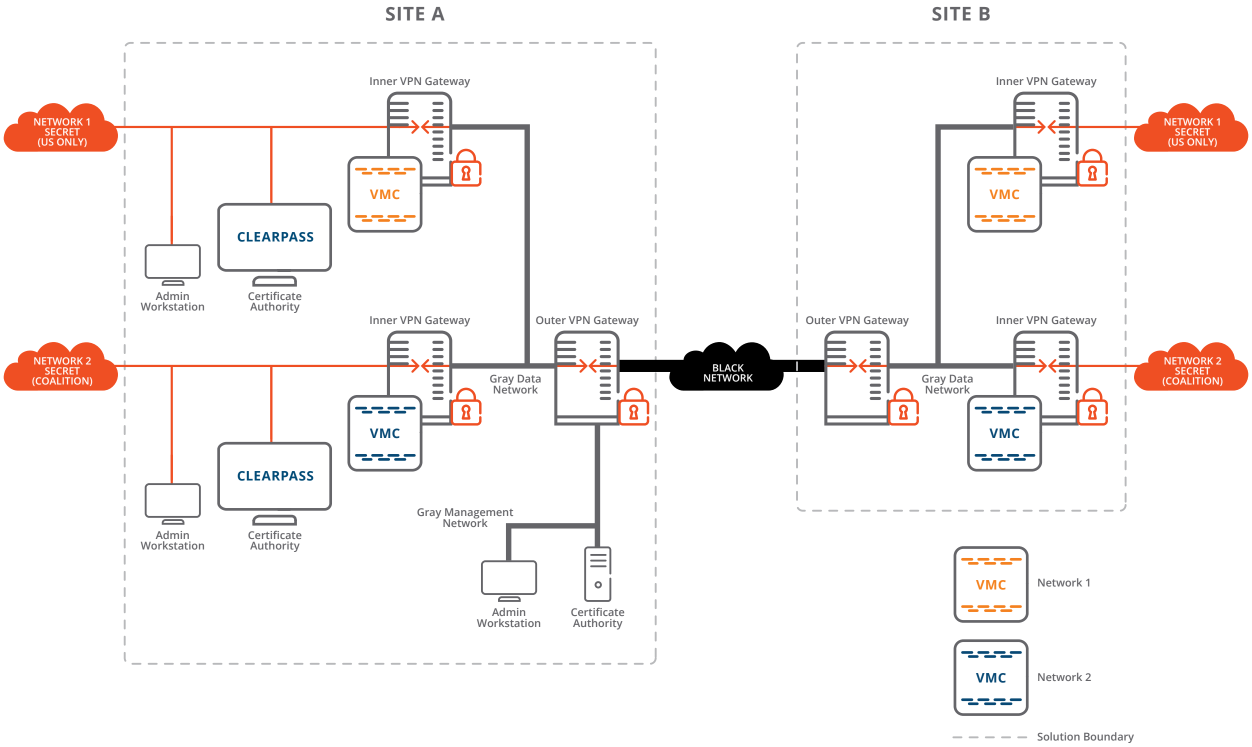


figure 28.0_100416_government-sga

Figure 28: Multiple Classification Site-to-Site

GOVERNMENT USE CASES AND SOLUTIONS

This section describes use cases specific to the government sector and outlines Aruba's solutions that address requirements specific to government agencies.

Primary Network Cost Savings

Given today's budget constraints, cost control and capital preservation is a key concern for every government agency. Historically, building out the wired LAN has contributed greatly to the excessive spending on network infrastructure. Local-area network design has largely followed the same methodology since the mid-1990s – hierarchically connected Ethernet switches in the core, distribution and access layers with every user connected to a single switch port. Over time, more cable drops have been added and more switch ports per user have been purchased as part of the standard configuration. Even with a shift to laptop systems for mobile computing, it is still common to install two to four wired ports for every user, connected by large multi-port switches and miles of cabling. A building with 1,000 users would require 4,000 ports, 4,000 cable drops, minimum of 100 Ethernet switches and untold maintenance fees.

Although it is well known that spending on wired connectivity is inherently inefficient, there has long been an absence of credible alternatives. However, Aruba's adaptive 802.11n/ac Wi-Fi technology allows the model to change, providing the performance, security and ease of management that enables administrators to reduce reliance on wired networks as the primary means of connectivity. Based on the Aruba Campus WLAN design, this particular solution involves a medium-to-high AP density deployment model and leverages the entire RF and security feature set of the Aruba architecture. The key goal is to reduce the number of Ethernet ports in the infrastructure and related cabling, switches and maintenance.

A single Aruba 802.11n/ac access point can support multiple simultaneous users at a cost of 10%-15% of a typical 48-port switch at list price. Aruba's adaptive 802.11n/ac technology may cost just 10% of a comparable wired build-out and can significantly reduce yearly recurring costs. The administration costs of adds/moves/changes disappear. Additionally, Aruba un-tethers users so they can work more productivity, roam freely, and collaborate more easily.

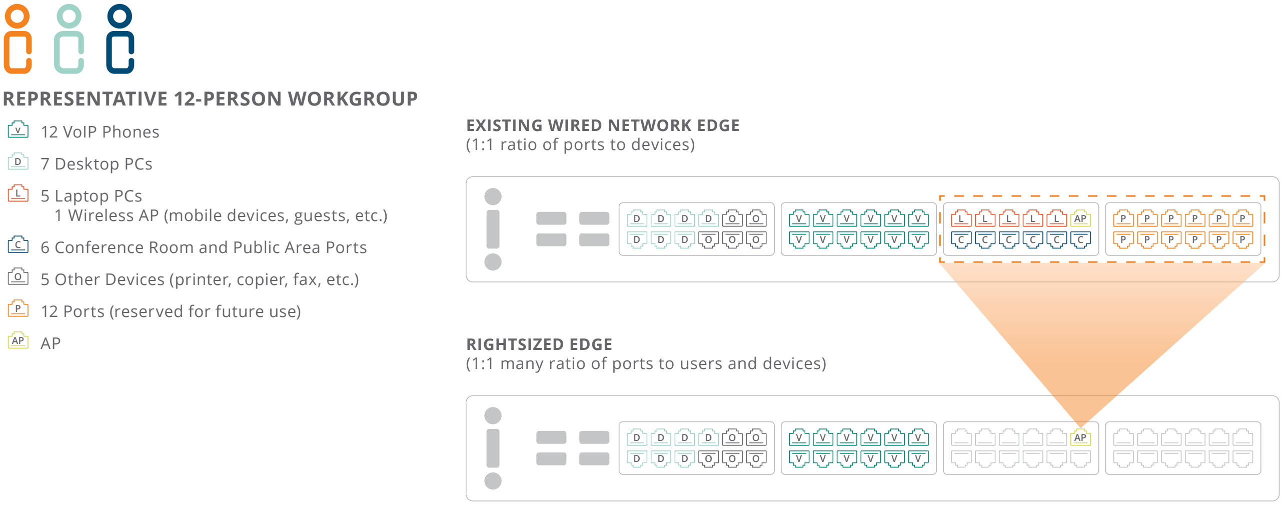

REPRESENTATIVE 12-PERSON WORKGROUP
V 12 VoIP Phones
D 7 Desktop PCs
L 5 Laptop PCs
1 Wireless AP (mobile devices, guests, etc.)
C 6 Conference Room and Public Area Ports
O 5 Other Devices (printer, copier, fax, etc.)
P 12 Ports (reserved for future use)
AP AP
EXISTING WIRED NETWORK EDGE
(1:1 ratio of ports to devices)
RIGHTSIZED EDGE
(1:1 many ratio of ports to users and devices)

figure 29.0_100416_government-sga

Figure 29: Cost Optimization through Ethernet Port Reduction Example

The following scenarios offer the best situations for network optimization:

- **Department moves/adds/changes:** These activities are accomplished faster and more economically when a WLAN is the primary access method and has the added benefit of minimizing port activation, deactivation and troubleshooting.
- **Access closet or IDF refresh:** This exercise presents an opportunity to audit port utilization, shift all mobile computer users to Wi-Fi to further reduce ports, and reduce closet hardware.
- **“Greenfield” deployment:** Bringing up a new building presents an opportunity to optimize the mix of wired and wireless ports from the outset, resulting in smaller closet switches, lower power consumption, and greatly reduced cabling.
- **Network expansion:** When increasing the network size, newer segments can be designed according to actual usage requirements, avoiding the higher costs of an overdesigned wired network in favor of a more economical wireless deployment.

Key Aruba features and benefits for this application include the following:

- Aruba’s 802.11n/ac access points are designed for 1.3 Gbps peak throughput
- Aruba’s identity-based security is more secure than wired connections
- Aruba’s multi-vendor AirWave Wireless Management Suite provides remote monitoring and problem resolution that is tightly integrated to the help desk

Logistics and Asset Management

Like the commercial world, many government agencies have the need to manage the flow of goods, information and other resources from point of origin to point of consumption. Wireless networks are critical to facilitating the transportation, inventorying, warehousing, and material-handling, as well as packaging of goods, machinery and data in a secure, most cost effective manner. These networks increase productivity by freeing workers from fixed workstations as well as paper notes and forms. Key requirements in a logistical or industrial environment include:

- Robust RF management
- Industrial-grade equipment built to withstand harsh environments
- Rapid deployment, even in areas where data cabling may be unavailable
- Support for a complex set of applications, including data acquisition and control systems, specialized handheld devices/applications and voice over WLAN
- No-compromise interoperability and security for low power, battery operated handheld devices from multiple vendors

Aruba’s unified mobility solution for logistics/industrial settings is built on the campus network design described previously in this document. This solution provides a secure, robust means of connecting mobile workers to the facility network and reliably delivering business critical applications no matter where users roam or the environment in which they work.

Wireless 802.11a/b/g/n/ac APs provide connectivity for bar code readers, laptops, hand-held devices, phones, and related mobile clients, linking them with multi-service mobility controllers over secure mesh, LAN, or WAN tunnels. Aruba offers a wide range of APs, from diminutively packaged devices that can be carried by traveling executives to explosion-resistant ruggedized units for harsh environments.

Aruba APs can be repurposed over the network, allowing one common SKU to service many applications. Configured as a remote AP, the device provides secure network access to roaming users – on the road, at remote sites, or at contractor facilities. Users gain access to the same network resources they would have at work, with the same level of security, but without the headaches of a managed client. Configured for secure mesh operation, the access points communicate wirelessly, and are a perfect way to signal over short or long distances without costly cable drops. Ideal for overcoming challenging installation scenarios, mesh is an invaluable tool where all-wireless signaling is a must.

Features and benefits of this solution include:

- **Purpose-built solutions for harsh environments:** Aruba’s ruggedized industrial wireless APs set the standard for robustness and flexibility, while the rich feature set accommodates a wide range of installation scenarios. They include a rugged IP68, NEMA UL 50 enclosure and wide operating temperature range permitting operation in physically and environmentally challenging locations. ATEX Zone 2 explosion rating, combined with fiber optic or wireless mesh operation, enables APs to be situated where standard commercial equipment cannot. Flexible power options – including solar panels, battery, high voltage AC, and Power-over-Ethernet – accommodate virtually any installation scenario.

- **Support for real-time applications:** Wireless networks must be continuously optimized in real-time to reliably support mobile voice, bar code scanning, inventory management and data terminal applications in the presence of a variety of noise and interference sources. Using standards-based mechanisms such as 802.1p and DSCP QoS tags, Aruba's networks monitor the type and traffic patterns of applications in use and automatically adjust parameters to ensure reliable application delivery.
- **Security without compromise:** Mobile manufacturing devices, unlike commercial laptop PCs, are often embedded computers with rudimentary WLAN security like WEP. Aruba's identity-based security securely connects these devices to the network and provides per-user firewall and wireless intrusion detection to protect against malicious activity and attacks.
- **Support for handheld and application-specific devices:** Mobile applications in the extended retail industry (retail stores, warehouses and factory floors) are unique in that they are not run on a traditional Windows-based device. On the contrary, mobile applications run on a wide-variety of application-specific devices (ASDs) that differ in form, input and output capabilities, operating systems, security capabilities, radio types and more. The use-case differences present a different set of "mobility performance" requirements on the mobility infrastructure such as fast roaming, load-balancing and battery life improvements. To support and secure a heterogeneous set of mobile device types, Aruba's architecture boasts a device agnostic approach. The Aruba solution follows an open standards approach and therefore does not require any proprietary client-side hook-ins or client side software to get full interoperability for delivering optimal "mobility performance."

Classified Networking Solutions Using Commercial Technology

Over the past decade, military, intelligence and critical civilian agencies have transitioned to "network-centric" applications to support their operations. The most important applications used by these agencies reside on tactically secret networks (i.e., the US Department of Defense SIPRNET), that have experienced a dramatic increase in importance and usage over the past decade. However, these organizations do not provide classified network access to all possible authorized users, and there are limitations on where this technology can be used, which severely hampers personal mobility. The under-utilization of classified resources is typically attributed to the expense of installing classified network connections that are certified – challenging the usability and cost of government-specific proprietary crypto systems (e.g. the US TYPE-1 system) as well as reports of low performance of SIPRNET access connections.

Due to these challenges, there is a desire to use commercial technology cryptosystems to provide classified network access due to the advantages found in using commercial solutions: high performance, lower acquisition and operations costs, and a rapid cycle of feature and product innovation. But the strength of the underlying crypto algorithms has simply not been robust enough to meet the stricter government communications security requirements. In addition, several of the older and widely deployed underlying cryptology methods found within commercial solutions are scheduled for government use de-certification due to the increased likelihood of exploitation.

Ultimately what is needed is a solution that features the characteristics of a commercial technology augmented with stronger underlying cryptography algorithms. Aruba, in conjunction with the NSA through its Commercial Solutions for Classified (CSfC) program, has developed an alternative access network architecture for classified network connectivity. This alternative architecture uses the collection of protocols and methods referred to as Suite B, and is intended to be easier to deploy and manage, has better operational performance and offers multiple access methods, including wired, wireless and remote access.

This solution conveys the following benefits:

- Improve classified network access to authorized personnel:
  - Enable mobility through high performance, classified-capable WLAN
  - Avoid the time and expense of physical hardened network connections
  - Expand classified network and application usage to larger user population
  - Lower cost to purchase
  - Lower cost to operate
- Enhance user adoption and satisfaction:
  - Improve individual user performance and overall classified network capacity
  - Reduce or eliminate use of Controlled Cryptographic Items that must be physically secured when not in use
  - Increase the number and flexibility of use cases and classified access mission profiles

- Future-proof the network architecture:
  - Elevate the overall communications security posture of new unclassified networks in anticipation of the deprecation of older crypto methods
  - Similarly, utilize classified-capable solutions when building new unclassified networks, in anticipation of elevating them to classified status at a later date
  - Operate truly unclassified networks at a classified level by using commercial technology

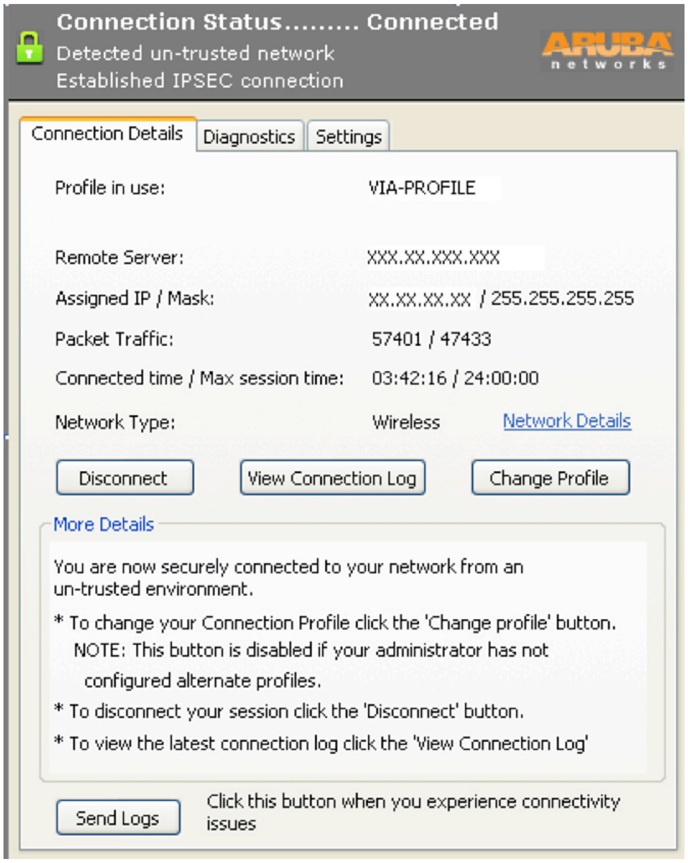
In order to protect these classified or other high-value networks from brute force attacks and other attack vectors, Suite B replaces or augments both the asymmetric cryptography algorithms (used, for example, during key exchanges) and symmetric crypto algorithms (used for unique user-session data encryption). The Suite B algorithms not only have a better overall crypto strength, but the underlying computation methods are more efficient, making them more appropriate for high-performance applications. Briefly, the Suite B protocols and methods required are:

- SHA-256/SHA-384 Secure Hash
- Elliptical Curve Digital Signature Algorithm certificates/ signatures (ECDSA 256/384)
- Elliptical Curve Diffie-Hellman for key exchange (ECDH 256/384)
- AES-128 and AES-256 user-data symmetrical cryptography, with the AES-GCM mode

Aruba's mobility controller hardware (7200 series, 6000 M3-Mk1, 3000 series and the 600 series) is designed to address these classified network access requirements by supporting Suite B.

Aruba's Virtual Intranet Agent (VIA) client also supports Suite B. The VIA client is a soft-installable NIC client driver/IP stack shim that detects whether the client device is connected to a trusted or un-trusted network, and then uses a combination of authentication and encryption to create a secure tunnel connection to its home controller. It can operate in either 802.11i WLAN Client Supplicant mode, in Ethernet LAN IPSec mode or in Remote Access IPSEC mode. All modes include the following protocols and methods:

- SHA-256/SHA-384 Secure Hash
- ECDSA certificates/signatures
- ECDH for key exchange
- AES-128 and AES-256 bulk symmetrical cryptography
- Support for all of AES-CBC, AES-CCMP and AES-GCM modes
- WLAN Mode: bSec (802.11i enhanced with Suite B) using EAP-TLS 1.2
- VPN Mode: IPSEC + Suite B using IKEv2


Connection Status......... Connected
Detected un-trusted network
Established IPSEC connection

Profile in use: VIA-PROFILE

Remote Server: XXX.XX.XXX.XXX

Assigned IP / Mask: XX.XX.XX.XX / 255.255.255.255

Packet Traffic: 57401 / 47433

Connected time / Max session time: 03:42:16 / 24:00:00

Network Type: Wireless Network Details

You are now securely connected to your network from an un-trusted environment.

* To change your Connection Profile click the 'Change profile' button. NOTE: This button is disabled if your administrator has not configured alternate profiles.

* To disconnect your session click the 'Disconnect' button.

* To view the latest connection log click the 'View Connection Log'

Click this button when you experience connectivity issues

figure 30.0_100416_government-sga

Figure 30: Aruba Virtual Internet Agent

VIA for Windows, Linux, and Android are already accredited for CSfC. Additional certifications will be achieved through other agencies in order to deploy this solution as part of a classified access network architecture. When combined together with other appropriate networking and security technologies, they are intended to provide a classified-capable access network connection for local LAN, WLAN and remote access requirements. Because this solution is based on commercial crypto technology, it will be available not only to US government agencies but to other defense, government and critical infrastructure organizations world-wide.

The advantages of this solution architecture include:

- **Enabling technology for new mission profiles:** Suite B will fundamentally transform mobility oriented communications due to a lack of Controlled Cryptographic Item issues, which affect salability outside authorized government agencies and exportability.
- **Support for all access modes:** The ability for the high-performance Aruba mobility controller to manage both classified WLAN users and classified wired users, thereby simplifying the network design and increasing overall security by adding access control and user firewalls for all users.
- **Multiple services on the same WLAN:** The ability to have both unclassified and classified access available in different or same coverage areas using a single WLAN network architecture. Physical separation of user traffic based on advertised network availability and logical separation of user traffic through the controllers crypto and user-firewall functions will ensure classified and unclassified traffic is not co-mingled.
- **Support for both local and remote users:** The ability to rapidly deploy secure access locally (using WLAN) and remotely (using Remote WLAN) using a single network architecture.
- **High performance:** The Aruba M3-Mk1 Controller supports 4Gb/s of AES-256 encrypted throughput that supports thousands of users simultaneously. Up to four modules can be installed into a single Aruba 6000 Controller chassis for 16Gb/s of encrypted traffic throughput.
- **Lower acquisition and operational cost advantage of a commercial solution** rather than a government/ proprietary solution.

Providing Guest Access via WLAN

Aruba provides multiple options for allowing guest access for wireless LANs, which can be customized based on the needed level of security or functionality:

- Simple “splash page” registration, whereby a user clicks to accept an acceptable use policy and is then given Internet access.
- Guest authentication based on a common access code that is known to employees and can be given to guest users.
- Self-registration over the Wi-Fi network, where users supply name, phone number, email address, or other details and are then given a unique username/password.
- Self-registration at a physical registration terminal, such as a guest check-in kiosk in a building lobby.
- Sponsored guest registration, where a visitor must supply the name of an employee who he/she is meeting. The sponsor must approve the guest registration by click on an email.
- Sponsored guest registration with the sending of a password to the user’s mobile phone through an SMS/text message. This provides the greatest degree of traceability since both the sponsor identity and the guest’s mobile phone number are known.

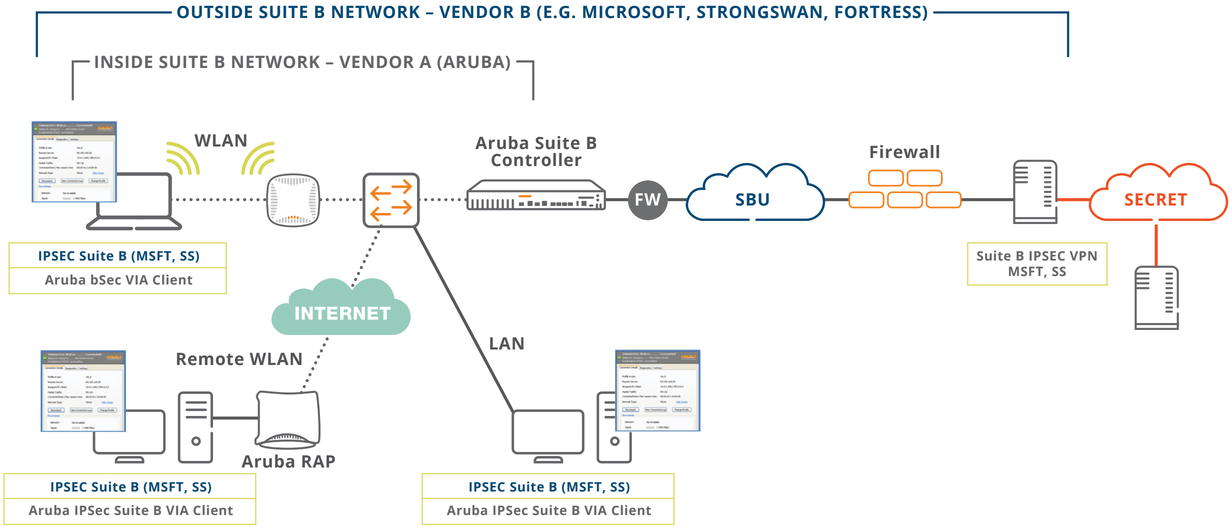

OUTSIDE SUITE B NETWORK – VENDOR B (E.G. MICROSOFT, STRONGSWAN, FORTRESS)
INSIDE SUITE B NETWORK – VENDOR A (ARUBA)
WLAN
Aruba Suite B Controller
FW
SBU
Firewall
SECRET
IPSEC Suite B (MSFT, SS)
Aruba bSec VIA Client
Suite B IPSEC VPN MSFT, SS
INTERNET
Remote WLAN
LAN
Aruba RAP
IPSEC Suite B (MSFT, SS)
Aruba IPSec Suite B VIA Client
IPSEC Suite B (MSFT, SS)
Aruba IPSec Suite B VIA Client

figure 31.0_100416_government-sga

Figure 31: Example Classified Access Architecture with Aruba Suite B

Aruba's ClearPass Policy Manager serves as the engine that enables customizable guest access services. ClearPass works in conjunction with Aruba mobility controllers to enforce appropriate access rights – for example, providing some guest users with heavily filtered and restricted guest access while others receive more open access. Another example would be providing bandwidth or time-limit controls for guest users. ClearPass also enables guest management features such as bulk creation of guest access credentials (sometimes called "scratch-off cards"), and tight integration with lobby registration kiosks.

Using Aruba's Common Criteria evaluated stateful firewall capability, guest traffic is guaranteed to be kept separate from non-guest traffic. Combined with Aruba's IPsec and GRE tunneling capabilities, guest traffic can even be transported across restricted networks such as the NIPRnet.

Mobile Device Internet Access through Restricted Networks – Tunneled Internet Gateway

Most mobile device users working in a government agency are restricted from accessing the Internet from non-policy compliant mobile devices. Aruba's Tunneled Internet Gateway is a productivity enhancing functionality that allows these mobile device users to connect to the Internet gateway through restricted networks that are normally off-limits without radical modifications to their device.

Enabled through software configuration of an Aruba controller-based WLAN, Tunneled Internet Gateway creates an encrypted data session between a mobile device and the Internet gateway on restricted networks, NIPRnet, or other networks that carry sensitive data. Through encrypted tunnels, authorized users utilizing commercial smartphones and tablets can connect to the Internet by accessing the restricted network to connect to the Internet gateway, usually located in the DMZ, or other location. ClearPass, either with its own user database, or by connecting to an external identity store, allows authorized users to connect to the WLAN and enter user credentials in a captive portal. All data between the controller and the client is encrypted; data cannot mix with restricted network data, and access to network resources is prevented by the firewall tied to the user's permission settings. Once traffic reaches the controller, it is re-encrypted and forwarded through an IP tunnel to a gateway on the commercial Internet.

Secure Telecommuter Access

Mobility in the government sector is increasing at an incredible rate with workers traveling around the country or working partially or fully at home offices. The typical mobile worker (often referred to as a "road warrior") is an employee who never sees the inside their office and who is only known by their voice and email. Some days the road warriors are working from home or in a temporary office; other days they are in hotels, airports or other Wi-Fi hotspots.

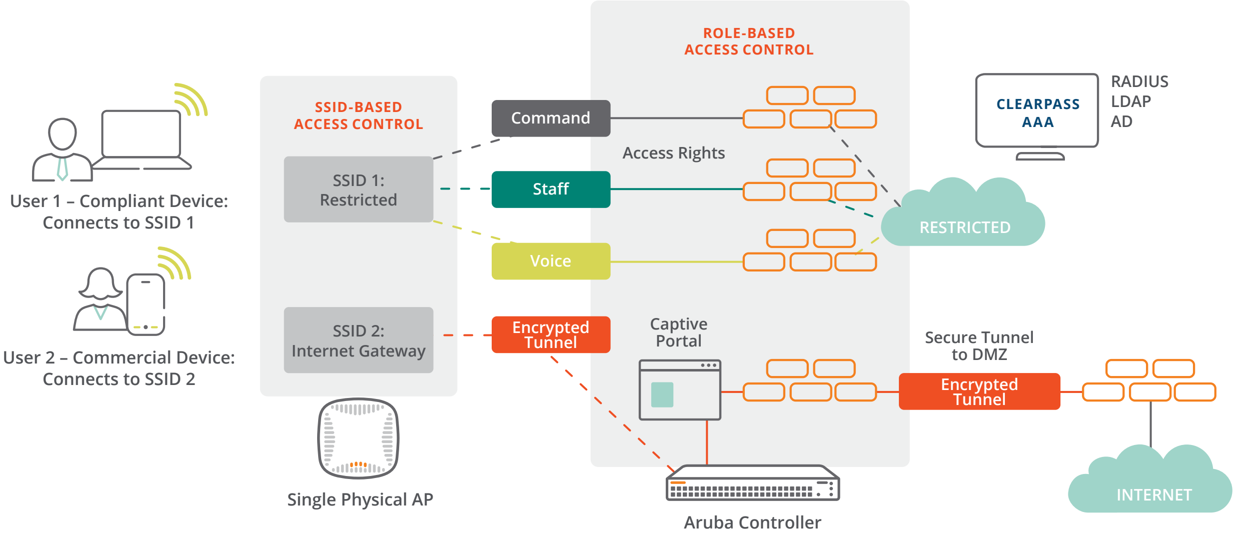


figure 31.0_100416_government-sga

Figure 32: Tunneled Internet Gateway

However, it is not only the road warriors that require remote access. In order to improve productivity many agencies have begun to provide permanent Home Office workstation setups for users that frequently extend their workday. Additionally, government administrators have found it cost effective to allow employees to work exclusively from home on a part-time or full-time basis.

Unfortunately, when any user leaves the office, productivity decreases due to lack of commonality in connectivity and remote access architectures for different devices. Various devices (web front end, VPN, SSL-VPN, etc.) are deployed for different use cases and it is not uncommon for problems to frequently occur with the access methods.

The solution for the telecommuter is based on Aruba's virtual branch networking solution described previously in this document. The architecture can vary slightly depending on specific need of the user.

- For fixed small office/home office locations, Aruba APs operating in Remote AP mode provide always-on secured wired and wireless connectivity for the telecommuter's laptop, wired VoIP phone, desktop computer or printer.
- Road Warrior: In a typical deployment, the road warrior has a setup that includes Aruba' Virtual Intranet Agent (VIA) client installed on their laptop to be used at all times. The VIA client allows this user to securely connect to the enterprise from any wired or wireless Internet connection. The VIA client will have a number of advantages over traditional VPN "dialer" clients, including:
  - The ability to dynamically detect when operating inside versus outside the agency network
  - Auto-detection of "un-trusted" network and automatic secure connection establishment
  - Dynamic transport selection between IPsec and SSL
  - Auto-upgrade configuration management
  - Auto-management of the Windows Zero Config for all wireless client configuration
  - Single point of policy enforcement from the Aruba controller
- Optionally, mobile RAP-3WN, RAP5WN, RAP-100 series, and RAP-155 series remote APs with USB-attached cellular modems provide a portable, always on connection to the agency network. This RAP can be used when in a location with Ethernet connectivity to the Internet (e.g. using a guest access connection or in a hotel) or on-the-go via the 3G/4G cellular modem. This portable RAP provides the same secure wireless/wired connectivity as the fixed-location home office RAP.

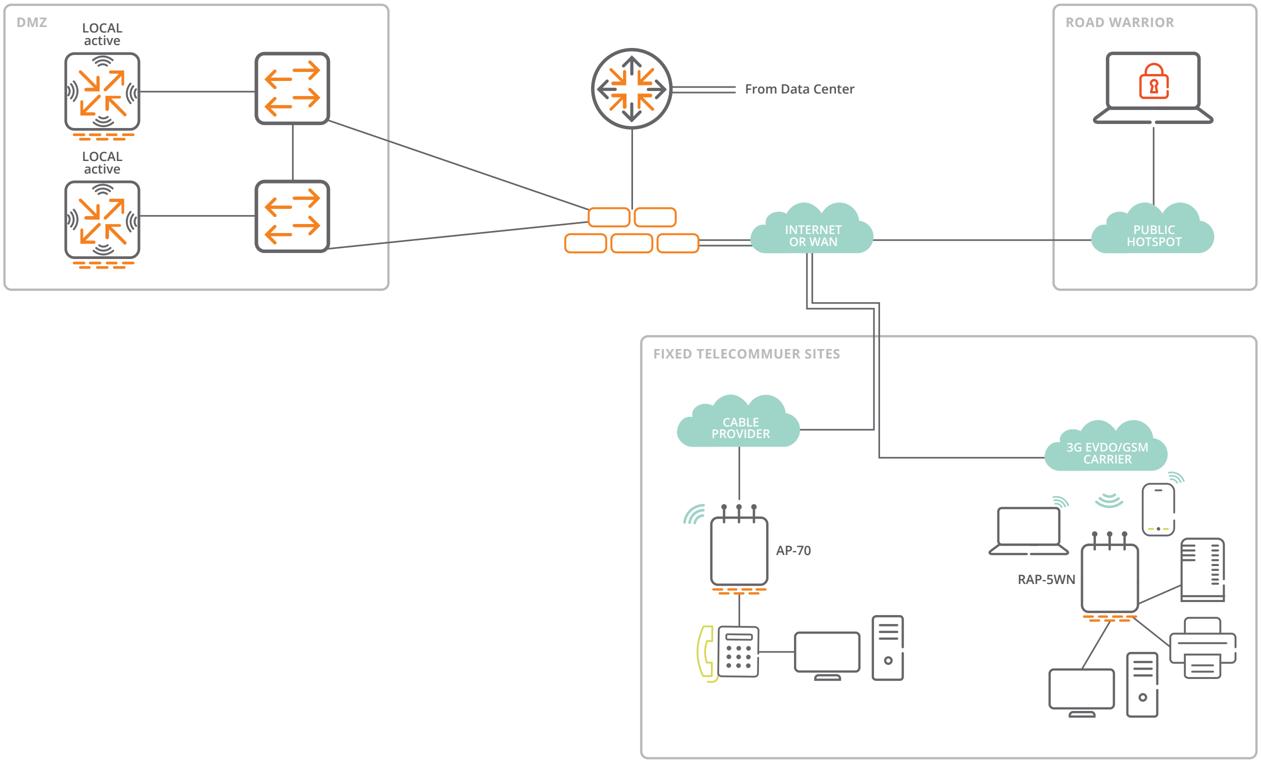


figure 33.0_100416_government-sga

Figure 33: Secure Telecommuter Access Example

Key features and benefits for this application include:

- **Zero-touch installs:** RAPs can be deployed without IT technicians touching any of the devices. The administrator simply configures a list of authorized RAPs on the controller, the end user enters the URL of the controller into a RAP Web browser and the rest is done automatically.
- **Automated local AP activation:** After the RAP is provisioned, it downloads the appropriate group profile configuration for the specific AP and goes live. The RAP then detects other local WLANs and sets its internal WLAN radios accordingly, automatically activates a secure connection for user traffic, activates Corporate SSIDs in the local environment and then detects and secures the attached wired devices.
- **Seamless application access:** Aruba's RAPs extend the agency/department network experience anywhere there is an Internet or cellular connection. Laptops, printers and wired VoIP phones work just as they do in the office – including internal phone dialing, fileserver access and applications access.
- **Resilient WAN connectivity:** Should a wired WAN link fail, a select range of RAP models can automatically switch to a 3G cellular modem for dial back-up.
- **Always-on connectivity:** Aruba's solution supports both inter- and intra-data center redundancy. The RAP does not need to be programmed individually with route information – it is capable of discovering alternative paths automatically. Optional split-tunneling can direct Internet-destined traffic away from the enterprise network and allow direct-to-Internet access for selected sites, users and devices.
- **Role-based access control and policy enforcement:** Both Aruba's controller and RAP have an integrated, authentication enforcement point and Common Criteria validated stateful firewall. Users are authenticated by the Agency RADIUS/Directory server and the RAP will then dynamically activate traffic management rules for each user. User policies that might normally only be present in the HQ LAN environment "follow the user" so they are active in the same way in the RAP network as well.
- **Single point of management:** All Aruba RAPs and VIA clients are managed from the one Aruba conductor controller and/or the Airwave Conductor Console for the entire VBN network. Code upgrades and configuration changes take place in this one location and automatically and safely propagate to all APs and clients without administrator intervention. Remote diagnostics and troubleshooting are also available from these single points of management ensuring rapid problem detection and resolution.

Workforce Displacement and Continuity of Operations (COOP)

Many government agencies have the need to support a large percentage of geographically dispersed workers for weeks or perhaps months at a time. These situations set up the following network requirements:

- Employee access to all communications and information systems from their remote location in a manner identical to their office experience
- Business partner or contractor access to specific information systems from a remote location
- Instant-on network that is highly portable
- Ability to connect via many different broadband Internet access methods

The Workforce Displacement solution is based on Aruba's Virtual Branch Networking (VBN) portfolio described previously in this document. This architecture provides secure, reliable remote networking for branch offices, at a price point that makes it feasible to deploy on a massive scale. One or more Aruba controllers of appropriate capacity are "hot staged" in a data center that will serve as a communications and info services hub. The controller is configured for remote access as its primary application, and is tied into various back-end systems for user authentication and management. Then by deploying inexpensive Remote Access Points (RAPs) or Branch Office Controllers (BOCs) in the remote offices, VBN creates a secure connection back to the data center over any wide-area transport, including 3G cellular, residential DSL and cable networks. Using Aruba's AirWave software, IT staff members can monitor and manage the entire network remotely for as long as required.

RAPs and BOCs support the centralized management of data, voice, and video applications, including wired voice over IP (VoIP) desk phones and wireless smart phones. Installation is plug-and-play user installable and features built-in diagnostics. Software updates are centrally disseminated, eliminating the need to manually upgrade hundreds or thousands of sites. Also, the Aruba VIA client can be used as a software alternative to a Remote AP providing secure connectivity from a laptop for a single user, such as a business partner or contractor.

This solution is instantly deployable – Aruba APs of various types can be pre-purchased, pre-provisioned and placed into a staging location for later distribution. APs can also be purchased "on- the-fly" and self-provisioned by the worker in their remote location. There is no software to install on the user's laptop nor are there any configuration changes required on the user's system or in the core network.

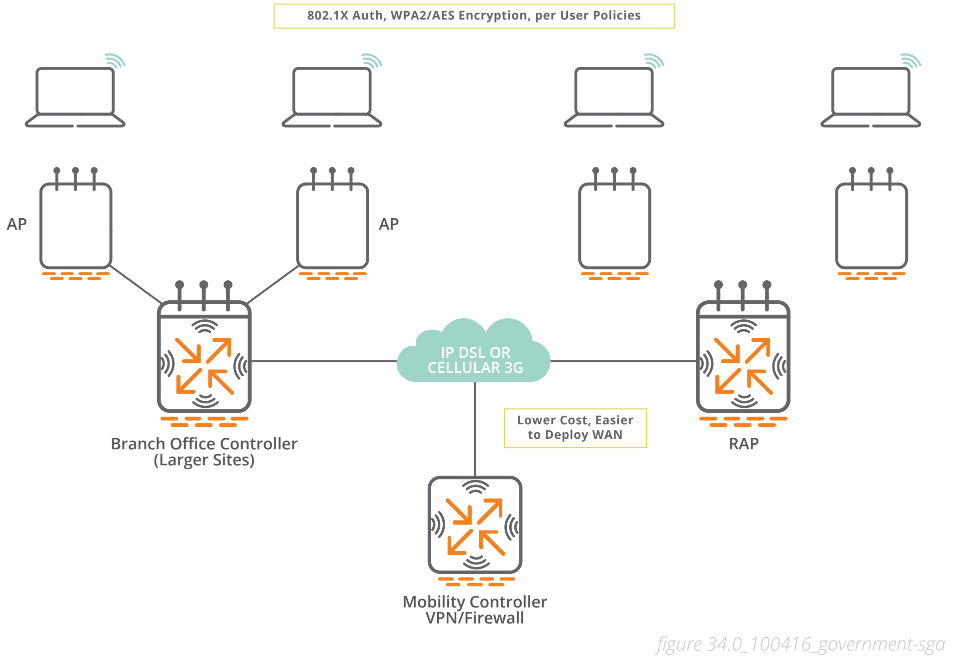

802.1X Auth, WPA2/AES Encryption, per User Policies
AP
AP
IP DSL OR CELLULAR 3G
Lower Cost, Easier to Deploy WAN
Branch Office Controller (Larger Sites)
RAP
Mobility Controller VPN/Firewall
figure 34.0_100416_government-sga

Figure 34: COOP Logical Design Example

Key Features and Benefits for this application are similar to those described in detail for the Telecommuter solution discussed in detail above including:

- Zero-touch installs
- Automated local AP
- Seamless application access
- Always-on connectivity
- Role-based Access Control and Policy Enforcement
- Centralized management, troubleshooting and reporting

TECHNOLOGY ADVANTAGES OF THE ARUBA SOLUTION ARCHITECTURE

Using the previously mentioned technology components, Aruba meets the following requirements for the deployment of secured applications over WLANs and remote networks:

Requirement 1: A High Performance Wireless LAN

Aruba APs can be deployed in a configuration that meets the environmental and performance requirements of the application. Any Aruba AP can be configured in any deployment mode: campus (Ethernet attached), mesh or remote. Single radio/dual radio, integrated antenna/external antenna, 802.11ac Wave 1 and 2 solutions are all available. Aruba's purpose-built APs provide the fastest WLAN throughput compared to competitive solutions, and all functions are fully configured and controlled in real-time by the centralized Aruba mobility controller. Configuration options limit the frequency bands/channels to those approved for the host country – ensuring all CONUS and OCONUS unlicensed frequency band guidelines can be met by a common architecture.

A key Aruba feature, Adaptive Radio Management (ARM), provides centralized RF management that eliminates the need for site surveys and proprietary single-channel single-MAC schemes. ARM has two purposes: maximize performance and minimize interference. To maximize performance, ARM implements features such as airtime fairness to prevent one client from monopolizing resources at the expense of another, automatic coverage hole detection to avoid RF dead spots and automatic load balancing to even out client load on APs and active RF channels.

To minimize interference, ARM performs detailed spectrum analysis on each AP and automatically adjusts channel plans and power settings to ensure appropriate coverage, mitigates interference in real time and manages co-channel interference to coordinate access to nearby APs on the same channel. Uniquely, ARM maintains full application awareness, allowing the administrator to designate application flows that should never be interrupted for RF management. The PEFng stateful user firewall also provides user and layer-7/application aware QoS controls for both the WLAN and the IP network attached, ensuring all user-application traffic is managed according to the policy priorities set by the agency. Additionally, bandwidth usage policies can be set to control how much WLAN bandwidth can be consumed by any single user or group of users.

High performance also means high-availability. Both the WLAN (via APs) and the controller can be deployed using a number of simple redundancy options to ensure a cost-effective but highly available WLAN solution.

Included with ARM 3.0, ClientMatch is compatible with all Aruba wireless APs. ClientMatch eliminates the sticky client problem where client devices remain connected to an access point, even though access points with a better signal may be available. As the sticky client moves further away from an access point, data rates decrease, negatively affecting network throughput. ClientMatch eliminates this problem by continuously gathering session performance metrics from mobile devices and steering clients to APs with better relative wireless signals. The result is higher throughput and better overall performance for all devices connected to the WLAN.

Requirement 2: A Secure Operating Environment

Ensuring the security of the WLAN deployment "air space" is paramount. The Aruba secure WLAN architecture offers advanced wireless intrusion detection and prevention software, which operates on the same AP, controller and management hardware/software as used for WLAN access. This allows for continuous monitoring and increased visibility of the airwaves with "hybrid" APs and sensors that are managed within the same infrastructure. Rogue AP/rogue client detection capability is one of many features of the Aruba wireless intrusion prevention system which provides the customer with an unparalleled wireless security solution. Wireless Intrusion Detection Services (WIDS) is a US DoD mandated requirement and an integrated WIDS solution minimizes the resources required to manage an additional solution. Optional additional sensors can be deployed to monitor for unauthorized cellular and/or Bluetooth device usage within the operating area. Aruba's APs, mobility controller, and OS were designed to protect themselves, protect the data transmitted over the network, and protect the keys and management system that run the network. Together they comprise an enterprise wireless LAN solution that is Common Criteria and UC-APL certified, FIPS 140-2 Level 2 validated, and Directive 8100.2 compliant.

Requirement 3: Advanced Network Security

Security functions (including crypto, access control and firewalling) are centralized in the controller making it possible to correlate every packet with an authenticated user identity and enforce access control on a per-user basis. Aruba's mobility controllers are designed around a multi-core network processor and multi-threaded OS that allows for dynamic re-allocation of resources between multiple functions as needed. This architecture features hardware acceleration of all centralized cryptography processing. For example, Aruba's 7200-series Mobility Controller supports up to 29Gb/s of AES crypto throughput and firewall performance at 9.5 million packets per second and 39Gbps of throughput.

In some alternative-vendor wireless networks, end-user communication encryption is performed in the access point. In this environment, sensitive keys and credentials exist on the APs, which are installed in unsecure physical locations where someone could tamper with the devices. This often requires installation of these APs into secure enclosures.

In an Aruba network, sensitive information such as user encryption keys remains inside the data center in the controller. In our opinion, AP-based crypto does not provide end-to-end encryption, as mandated by DoD Directive 8100.2 – because encryption ends at the AP, not the core of the network. This mandate has forced some organizations to deploy "overlay cryptography" solutions to ensure FIPS, UC-APL and/or DoD directives compliance, which in turn increases complexity and causes significant design challenges and awkward end-device behavior.

Aruba's identity-based security establishes protection based on user-centric information instead of port-centric network access. By uniformly enforcing these policies regardless of where a user enters the network, security can be assured for mobile users without constraining how and where they roam. Role-based access can therefore be applied to a single SSID, used for NAC, applied to both wired and wireless networks, and delivers comprehensive access control (integrated firewall; time, location, and service policies; linkage of guest usage to internal groups; bandwidth management; secure traffic tunneling to DMZ; customized login page; active directory integration; usage audit reports).

Uniquely, Aruba includes a Common Criteria validated high performance, stateful policy enforcement firewall built into the mobility controller which is used to create interior enclaves and enforces inter-user and inter-department network security policy. Aruba's firewall takes preventive actions dynamically against internal security breaches and attacks, and features L4-7 awareness. Since the firewall is application aware using deep packet inspection, it provides better security than the simple access control lists (ACLs) offered by other solutions. Aruba's firewall also ties into voice features like call admission control, application-aware RF scanning, and per-application QoS enforcement. Competing vendors that do not offer stateful packet inspection cannot provide these services on a per-application basis.

Requirement 4: Easy to Deploy, Monitor and Manage

Aruba's controller software platform, ArubaOS, follows three principles:

1. **Centralization** of functionality that simplifies management and increases security.
2. **Flexibility** with regard to adding services providing investment protection.
3. **Integration** of network services enabling customers to deploy fewer physical products with a corresponding reduction in capital and operational expenses.

The mobility controller has all required deployment and monitoring functions necessary for any scale WLAN, available via secure user interfaces. APs are automatically configured by the controller at power-up, and are dynamically managed in real-time by the controller as conditions change. APs can be repurposed via over-the-network software downloads for access, wireless intrusion detection (WIDS), mesh and remote access.

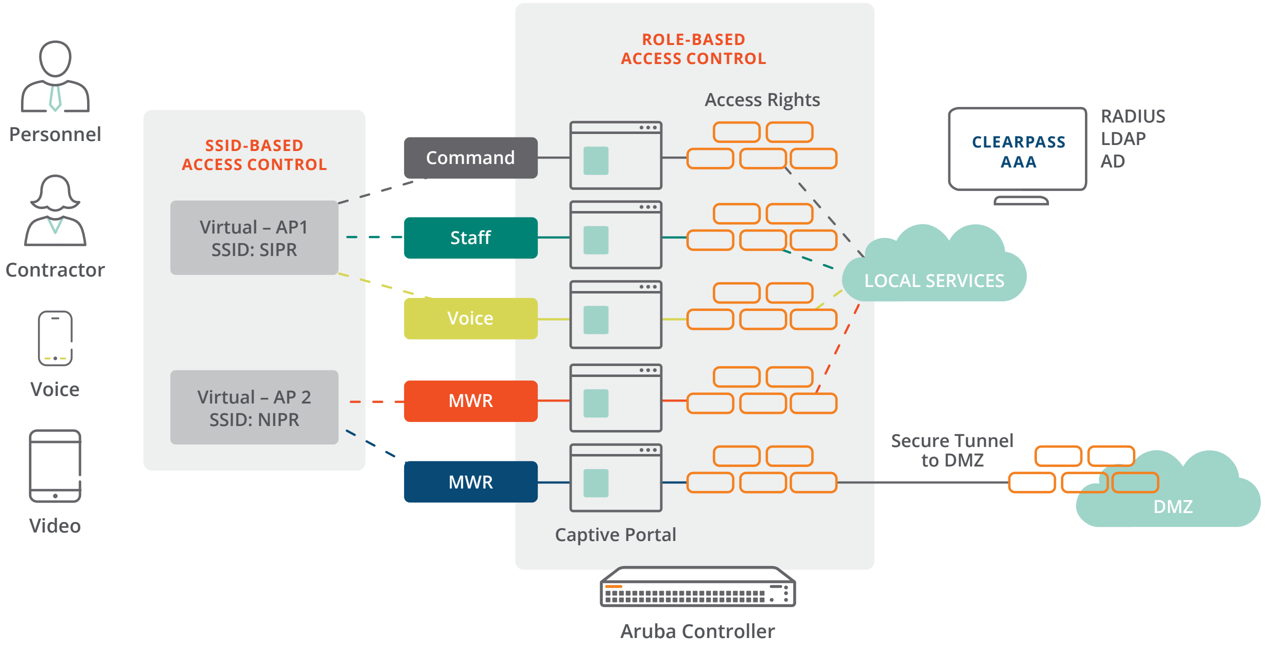


figure 35.0_100416_government-sga

Figure 35: Identity Based Access Control and Traffic Policy Enforcement

AirWave provides a single pane of glass to monitor and manage Aruba and other third party wired and wireless systems. It provides advanced WIDS functionality, UCC performance metrics, and end-to-end troubleshooting of the wireless network. With the addition of Clarity Live, Airwave can now identify and track performance metrics that affect wireless client performance but are symptoms of upstream failures (DNS and DHCP response times, authentication failures, etc.).

Requirement 5: Rapid Validation and Accreditation

Aruba is one of the few technology vendors that IA professionals fully support as being well-secured. By centralizing cryptographic functions on the controller rather than WLAN access points, sensitive information is never stored on products that are installed in physically insecure locations. Centralized crypto, combined with integrated user access control, user-level firewalling and WIDS makes Aruba's WLAN solutions more secure than many wired networks. We believe the comprehensive security capabilities and the technology validations current to the architecture will allow any DoD or other government organization to achieve an ATO.

Requirement 6: Expandable, Future-proofed Architecture

The Aruba architecture allows customers to build small point WLANs all the way up to centrally managed, global WLAN deployments and remote networks. Aruba solutions are used to build WLANs, Secure Remote Access networks and mesh networks – all from the same architecture, products and features. Unlike other architectures which have limited features or offer different capabilities that are hardware dependent, every major feature within ArubaOS runs on every Aruba controller and every Aruba AP – including: Wireless Intrusion Protection Services (WIPS), PEFng, mesh, remote networks, VPN, voice services, ARM, and Clarity. Aruba ultimately believes wired networks are less secure than wireless and thus do not offer the mobility and application flexibility found in wireless. We believe that government organizations will begin to deploy many different application services running on a pervasive global, mobile, highly secured distributed WLAN infrastructure. Aruba is the only vendor currently capable of delivering such an integrated WLAN architecture.

Additionally, Aruba offers a Virtual Mobility Controller (VMC) that provides the same features and functionality of the hardware products but in a software-only package. VMC is currently offered to DoD and other US Government customers for tactical and other battlefield-centric use cases where size, weight, and power (SWAP) are of utmost concern. VMC, when combined with other software services and applications on a VMware Hypervisor, offers a portable, end-to-end, security and application stack to meet tactical mission needs.

TECHNOLOGY REFERENCE

Current ArubaOS Standards, Government Certifications and IA-Validations

The following is a summary list of Aruba standards, certifications and government validations:

Relevant Standards

- Wi-Fi Alliance 802.11ac
- Wi-Fi Alliance 802.11n
- Wi-Fi Alliance 802.11a
- Wi-Fi Alliance 802.11 b/g
- Wi-Fi Alliance WME Certification for QoS
- AES-128/AES-256 CCMP; AES-GCM
- 802.11i/WPA2/xSec
- 802.1x including CAC card support

Information assurance validations

- ICSA Certified Stateful Inter-User Firewall
- FIPS 140-2 Level 2 for ArubaOS v6.5.0 FIPS
- FIPS 140-12 Level 1 for ClearPass Policy Manager
- FIPS 140-12 Level 1 for AirWave
- Commercial Product Assurance (CPA) as an IPsec Security Gateway (U.K.)
- Common Criteria VPN Client PP – VIA 2.3
- Common Criteria WLAN PP (AOS controllers and APs)
- Common Criteria NDPP+Firewall+VPN Gateway (AOS controllers)

Department of Defense

- NSA Commercial Solutions for Classified
- DoD Directives 8100.2, 8500.1, 8420.1 Compliant
- Unified Capabilities – Approved Products List (UC-APL) Listed
- DDR1494 JF12 Equipment Radio Frequency Allocation Guidance
- TAA Compliant

CITS / USAF

- ATO for USAF CITS 2GWLAN
- I-TRM purchase list

ARMY

- US Army Information Assurance Approved Products List for 802.11a/b/g/n Campus WLAN, Outdoor WLAN, Mesh WLAN, Remote Access, WIDS
- US Army Technology Integration Center (TIC) tested (passed)
- US Army Type Accreditation

NATO

- NATO Information Assurance Product Catalogue (NIAPC) Listing

JMIS TIMPO/NAVY

- IATO from JMIS and NAVNETWARCOM
- Navy HERO certification

Department of Homeland Security

- DHS Continuous Diagnostic Mitigation for Phase 1 Hardware Asset Management (HWAM)

Military Health System (MHS)

- ATO for all MHS facilities

Voluntary Product Accessibility Template (VPAT)

- Section 508 Compliant

a Hewlett Packard
Enterprise company

Contact Us Share