

Enterprise



Virtual Branch Networking

Introduction

Branch offices, satellite clinics, teleworkers, temporary workers, and traveling employees all require access to business-critical data from the enterprise 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 burdensome 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. Remote users often lack a full suite of network services such as printing, voice, and collaboration. Finally, port-centric management tools offered by vendors typically lack visibility into, and simple control mechanisms for, remote users.

Aruba's Virtual Branch Network (VBN) solution dramatically simplifies the complexity and cost of deploying a remote solution at branches with one to many users. Complex configuration, management, software updates authentication, intrusion detection, and remote site termination tasks are handled by powerful data center-based Aruba controllers running new Aruba software. Services are virtualized in the data center controllers and then pushed to low-cost, purpose-built remote access points (RAPs) and branch office controllers (BOCs). RAPs and BOCs provide secure connectivity and deliver centralized services to end users. Layer 3 tunneling between the controllers and RAPs and BOCs allows any wide-area network - including 3G cellular and DSL – to be employed.

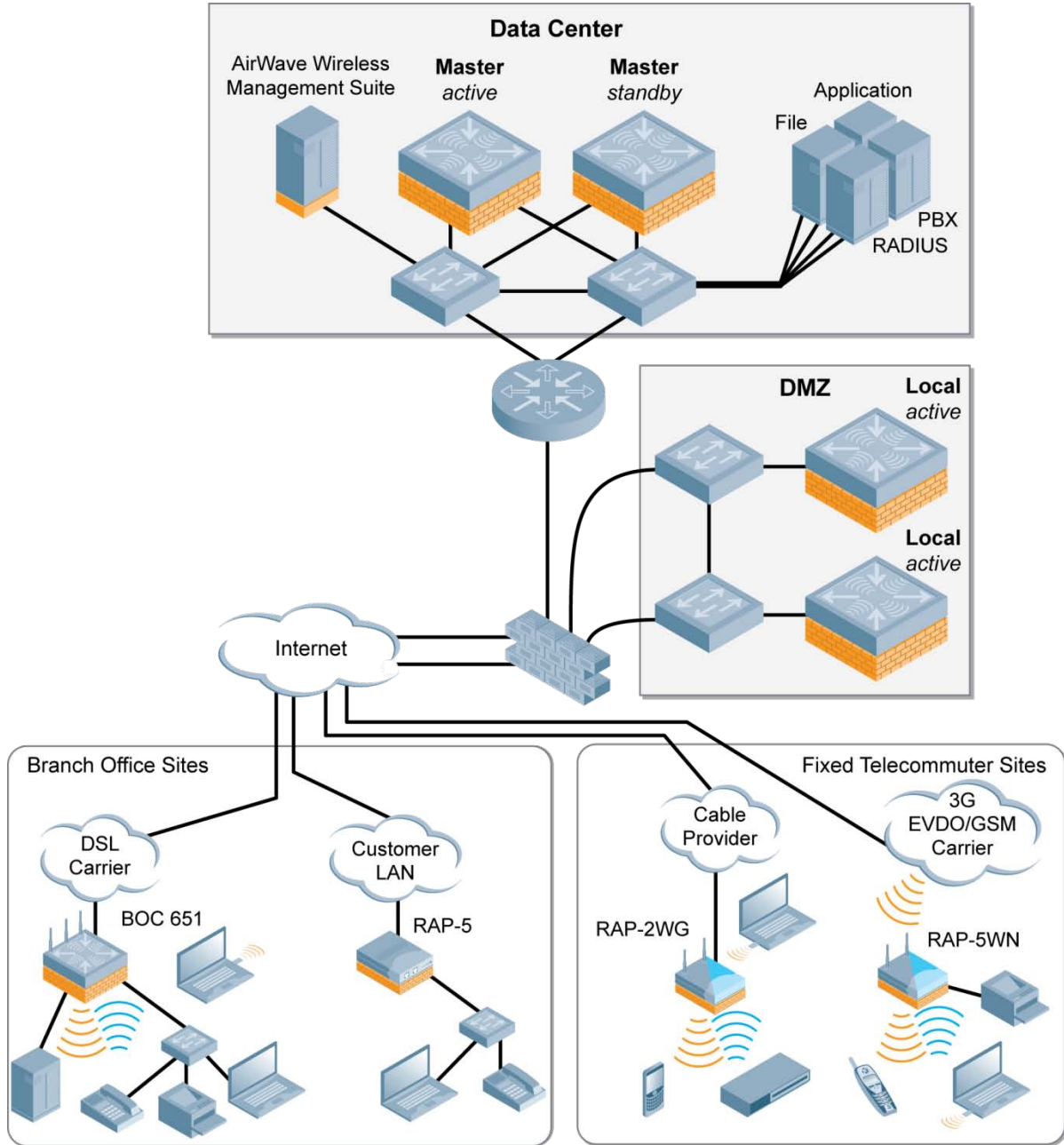
The VBN solution differs from traditional infrastructure solutions by focusing on policy instead of ports, routing, subnets, and VLANs. Aruba's distributed policy enforcement firewall provides a centralized way to manage and control policies, and dissolvable firewall agents that enforce policies in the remote devices. The firewall delivers policy-based control, high security, support for differentiated services based on user-type, and is always under IT control. The solution is persistent, easily configured, requires no user training, and delivers a plug-and-play experience. The result is a more uniform and secure user experience, regardless of where the network is accessed.

Unlike client VPN solutions, no special client software is required for remote access. There is no need to train users on remote access procedures, no software to launch, and no token cards to remember to use. Data are encrypted and authenticated, just like a VPN, but the user doesn't need to intervene to set-up a connection. All policies are uniformly enforced regardless of where the network is accessed, delivering the same user experience over both wired and wireless networks.

The VBN solution is managed by Aruba's AirWave Management Platform (AMP), which provides interfaces for the Help Desk, network engineering, security and audit groups, executive management, and the general user population. Unlike traditional network management solutions that focus on troubleshooting ports, VLANs, and IP addresses, AMP provides visibility down to the end user and device.

Key features of the VBN solution are designed to ameliorate the pain points of traditional remote networking solutions:

- The zero-touch IT provisioning model seamlessly joins a remote branch to the corporate network without additional log-on credentials or software to launch. A non-technical person can provision a wired and/or wireless RAP office without IT assistance. Applications and devices work out-of-the-box without additional configuration;
- 1-button debugging data generation, 1-button “reset” to defaults, and an intuitively simple user interface to speed problem detection and resolution;
- Bulk-provisioning allows credentials to be assigned automatically by the system – reduces IT credential management;
- Policy-based forwarding ensures that IP-based devices (VoIP phones, printers) and services work as well remotely as they do locally without a need for separate voice networks and related security infrastructure;
- Any commodity transport can be used in lieu of costly private networks;
- All management and control functions are centralized in the Aruba controller. This user-centric management architecture provides visibility to all users and devices, speeding fault isolation in the event of a problem – no separate management infrastructure is required;
- Centralized policies and user access control eliminates the need for secondary firewalls to protect the remote networks.



Aruba's Virtual Branch Network Solution

Purpose-Built RAPs and BOCs

Aruba has three purpose-built families of RAPs and BOCs. All of the devices offer policy-based local and remote packet forwarding, and Adaptive Radio Management (ARM) technology for optimized Wi-Fi operation. A diagnostics feature displays status on a simple user interface, and provides one-button debugging and one-button reset to factory defaults. Other key features of the new product families include:

- **RAP-2 Family:** No larger than a deck of playing cards and designed for use by 1 to 5 users, the RAP-2 is ideal for teleworkers, micro-branches, and SOHO applications. An 802.11b/g Wi-Fi radio and two Ethernet ports for use with wired devices, such as VoIP phones, are provided;
- **RAP-5 Family:** the book-sized RAP-5 includes 5 high-speed Ethernet ports, a USB port for a broadband 3G cellular modem, hardware accelerated encryption, and, optionally, an 802.11n Wi-Fi radio with integrated antennas. The RAP-5 family is designed for micro-branches with up to 50 users;
- **600 BOC Family:** designed as a “branch-in-a-box” solution for offices with up to 256 users, the 600 family offers a broad range of WAN connectivity, network-attached storage, integrated print server, gigabit Ethernet, power-over-Ethernet Plus (PoE+), ExpressCard® slot, and USB options. An optional 802.11n Wi-Fi radio is available with resilient mesh networking to enable a truly all-wireless office.



Aruba's Virtual Branch Network Line

RAPs were developed for small branch offices, telecommuters, SOHO applications. Secure one-click provisioning allows end users to commission a RAP with no assistance from IT, lowering both deployment and Help Desk expenses. One button diagnostics and one button restoration to factory default settings minimize the need to return a RAP to IT for diagnostics or reconfiguration.

RAPs incorporate Aruba's powerful Adaptive Radio Management (ARM) technology to automatically optimize wireless network performance without administrator intervention. Many RAPs support 3G cellular for use as the primary or back-up WAN, enabling an instant branch office

Software upgrades and configuration changes are pushed automatically to all RAPs by the controller, ensuring they are up-to-date at all times. RAPs that are off-line at the time of an upgrade will be updated the next time a connection is made.

The Aruba BOCs were developed for small to medium sites with up to 256 users. Connectivity is provided to wired and wireless users through high-speed wired LAN ports, Aruba wireless access points, and an optional integrated 3x3 MIMO 802.11a/b/g/n access point. In offices that use Wi-Fi, a BOC can manage other Aruba access points and incorporates ARM technology for best-in-class wireless performance.

BOCs can host USB printers and network attached storage. 3G cellular can be used for back-up WAN connectivity via USB or ExpressCard® slots. BOCs include an integrated authentication server for self-contained operation at small sites, though they can also leverage data center AAA resources.

Secure guest access is provided by Aruba's GuestConnect feature which allows non-administrative users to add temporary guest access accounts and print guest user instructions. As with RAPs, BOCs can be centrally managed either directly from an Aruba controller or from the AirWave Management Platform.

Zero Touch IT Deployment

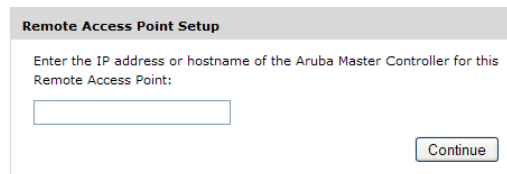
RAPs can be deployed without IT first touching any of the devices. The administrator simply configures a list of authorized RAPs on the controller, and when a RAP connects and presents a digital certificate that matches the authorized list it will automatically become part of the enterprise infrastructure. The end user need only enter the URL of the controller into a RAP Web browser, and the rest is done automatically. Configuration and software updates will be automatically loaded and updated in real time as configuration changes are made.

A set of instructions for the end user will be generated automatically by the controller and can be saved as a PDF. The instructions walk users through the provisioning process and can be e-mailed or printed and mailed to users.



The image shows the Aruba Networks Remote Access Point Provisioning interface. On the left is the Aruba Networks logo. To its right is the title "Remote Access Point Provisioning". On the far right, a box displays device information:

Device -----		Uplink -----	
Type:	RAP-2WG	Interface:	Port 0
Wired MAC address:	00:0B:86:C3:59:E6	Link Status:	UP
Serial #:	AH0000580	IP address:	192.168.1.103
Software Version:	ArubaOS Version 3.3.2.11-rn-3.0	Port speed:	100Mb/s



The image shows a "Remote Access Point Setup" dialog box. It contains the following text: "Enter the IP address or hostname of the Aruba Master Controller for this Remote Access Point:". Below this text is a text input field. At the bottom right of the dialog box is a "Continue" button.

RAP Self Provisioning Screen

Zero touch deployment is currently available on the RAP-2WG, RAP-5WN, and RAP-5 models supported by the Aruba 3200, 3400, 3600, and 6000 M3 series controllers.

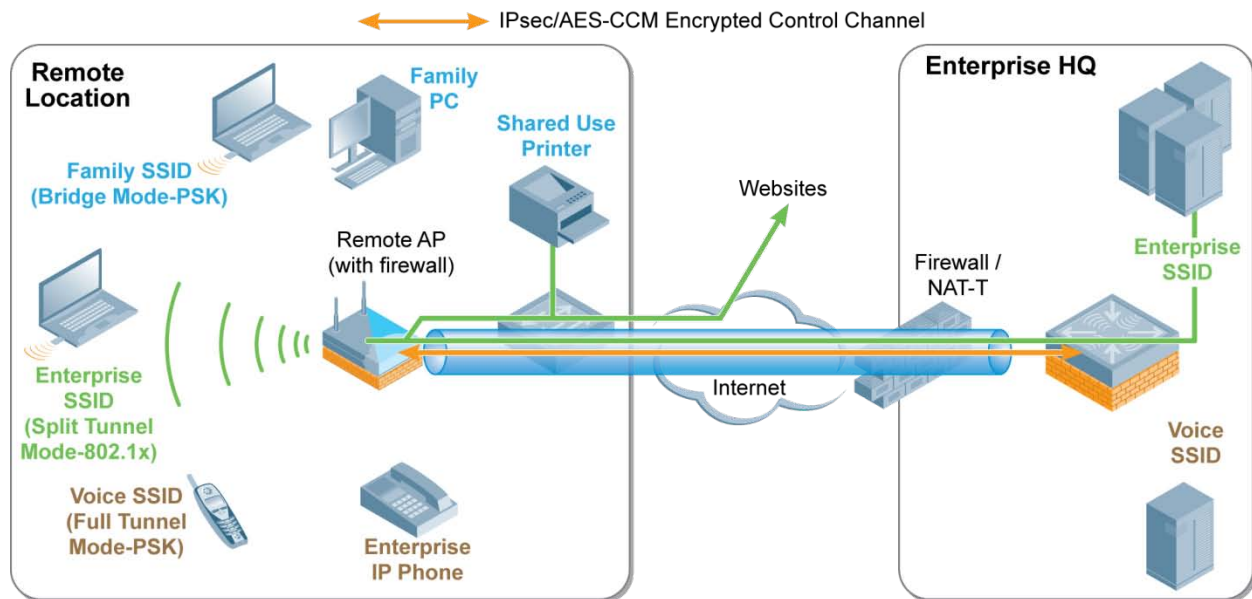
Policy Based Networking

Aruba's VBN solutions rely on policy-based configuration instead of port based security found on traditional solutions. Policies are managed by IT via the Aruba controller and then pushed automatically, without manual intervention, in near real-time to the remote devices whenever changes are made.

Policies can be used to define user roles, port behavior, SSIDs, traffic forwarding, authentication, and encryption. User roles are defined by firewall policies that define, on a user-by-user basis, which traffic types and resources users are allowed to access. As a result, multiple users can connect to the same RAP or BOC, using the same authentication method, and receive different access rights based on their IT-defined role.

LAN ports can be configured for open access or for authenticated network access control (NAC) mode, and can be configured for multiple authentication types. To enable employee and guest access on the same LAN port, 802.1X authentication and captive portal can be used simultaneously. Authorized users will be authenticated and given employee access, while guest users and non-802.1X devices will see a Web-based portal and must supply login credentials before access is granted. By enabling employees, guests, and unmanaged devices to share the same port yet have different access levels, Aruba does away with training users to use specific ports and security holes caused by unrestricted LAN ports.

RAPs and BOCs simultaneously support multiple wireless SSIDs on the same radio through the use of "virtual APs", allowing authentication and encryption to be customized on each SSID. For example, authorized users could utilize a full WPA2-Enterprise encrypted link, guests an open wireless network with captive portal for authentication, and VoIP phones a third WLAN using pre-shared key authentication, with all three existing on a single AP radio.



A RAP Operating with Policy Based Forwarding

Universal Connectivity at All Locations

Aruba's VBN solution allows common port configurations and/or SSIDs to be broadcast from all RAPs and BOCs simultaneously, effectively extending a single corporate LAN and WLAN to all remote locations. This feature enables laptops, Wi-Fi phones, PDAs, and other clients to recognize the network and connect automatically, using a standardized set of security protocols, regardless of the physical location.

All services are available at all locations with access strictly controlled by IT policies enforced by Aruba's firewall. Mobile users can enjoy the same access procedures and network services everywhere they connect to the network, while IT managers no longer need to carefully plan what services will be available to what users at different sites. No client software or token cards are required for access, and no workflow changes need to be made – security is completely transparent.

To further simplify network deployments, RAPs can extend IP addressing from the corporate site so that end stations operate in the corporate IP range. This reduces or eliminates the need for routing in the WAN because all IP addressing is "owned" by the data center-based controller.

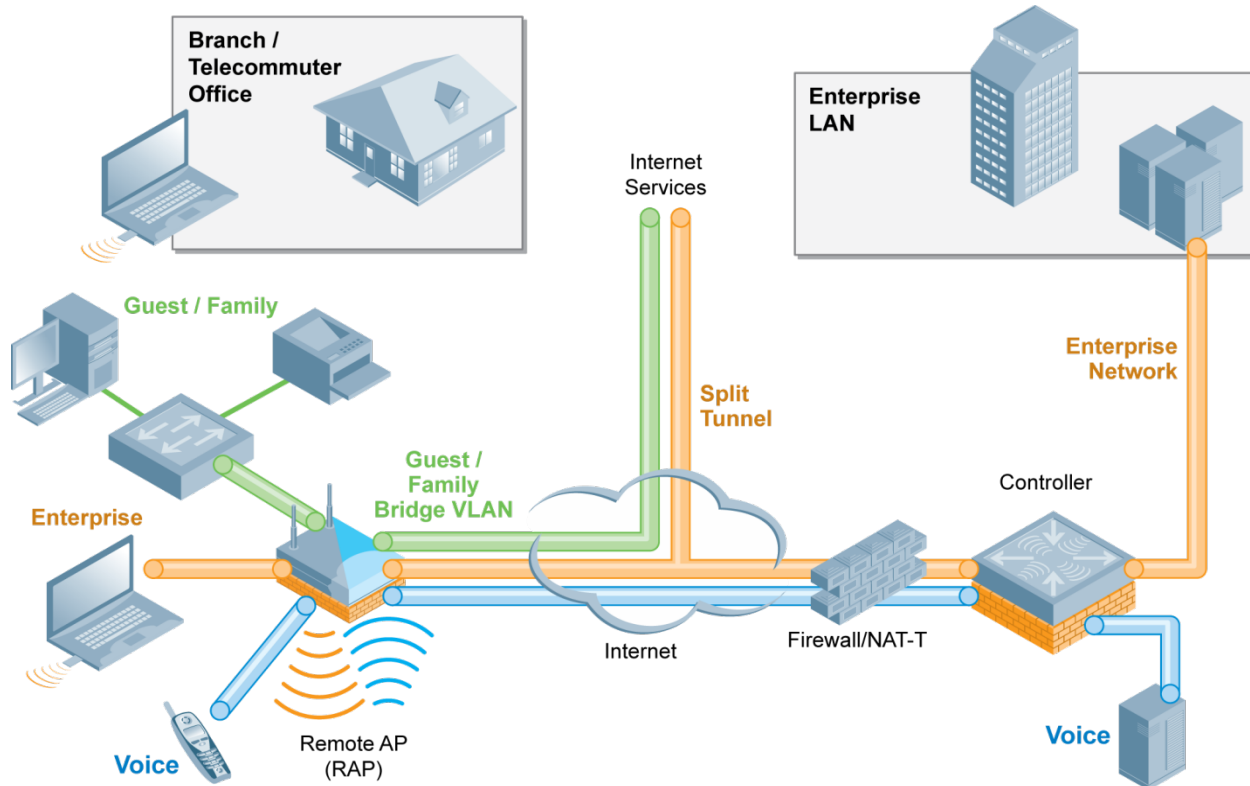
Reducing WAN Traffic Backhaul with Policy Based Forwarding

Optimizing WAN traffic preserves bandwidth for essential traffic and can lower operating expenses by allowing lower capacity, less expensive WAN connections to be used. Many traditional branch networking solutions pass all network traffic over the WAN to the data center for analysis. Internet traffic and local printer services often must be u-turned at the data center and sent back over the WAN, a time- and bandwidth-consuming process.

Aruba's VBN solution puts traffic forwarding control in the hands of IT. Running inside dedicated hardware using IT-defined policies, Aruba's Policy Enforcement Firewall (PEF) makes decisions based on IP address, type of traffic, and the policy associated with a user's role. Traffic destined for the campus office can be routed over a secure tunnel to the data center, while local or Internet-bound traffic can be locally bridged based on policy settings. Printing can be restricted to a local subnet. In contrast to VPN client "split tunnel" configurations, which can be manipulated by malicious software to forward between public and private interfaces, PEF ensures that policy decisions are always enforced.

While a router only examines the destination IP address of traffic and requires the configuration of complex access control lists (ACLs) to change forwarding and port behavior, PEF policies define security and traffic forwarding rules, and those policies are tied to specific users or devices and not to ports or VLANs. A VBN solution is simpler to configure and modify than a router-based solution, lowering the burden on IT not just at the time of deployment but also by eliminating adds/moves/changes through user based policy.

Access to a local network or to the Internet can be allowed via a policy, without interrupting a user's work flow. A traditional VPN client software solution, in contrast, requires that the user break existing connections, access the local resource, and then re-launch the network services – a major disruption and one that often results in time-consuming Help Desk calls.



Policy Based Forwarding

Keeping the Lights on with Site Survivability

Aruba provides two methods to keep a branch office up and running in the event of a WAN failure or a service interruption with the data center: 3G cellular back-up and local survivability mode. Should a wired WAN link fail, a select range of RAP and BOC models can automatically switch to a 3G cellular modem for dial back-up. The cellular modem plugs into a USB or ExpressCard slot on the RAP or BOC, allowing for a wide range of modems and service providers.

Local survivability mode maintains local LAN and wireless LAN access during a data center service interruption. This feature maintains intra-site communications and, depending on the status of the WAN and IT policy, Internet access as well.

Aruba controllers in the data center can be clustered for high availability, and DNS based techniques can be used to enable data center redundancy as well.

Simplifying and Securing Remote Wireless Deployments

VBN fits seamlessly into Aruba's end-to-end wireless security and manageability. Deploying wireless at the branch is simplified as all RAPs and BOCs support Aruba's wireless intrusion prevention system (WIPS) and Adaptive Radio Management (ARM) software.

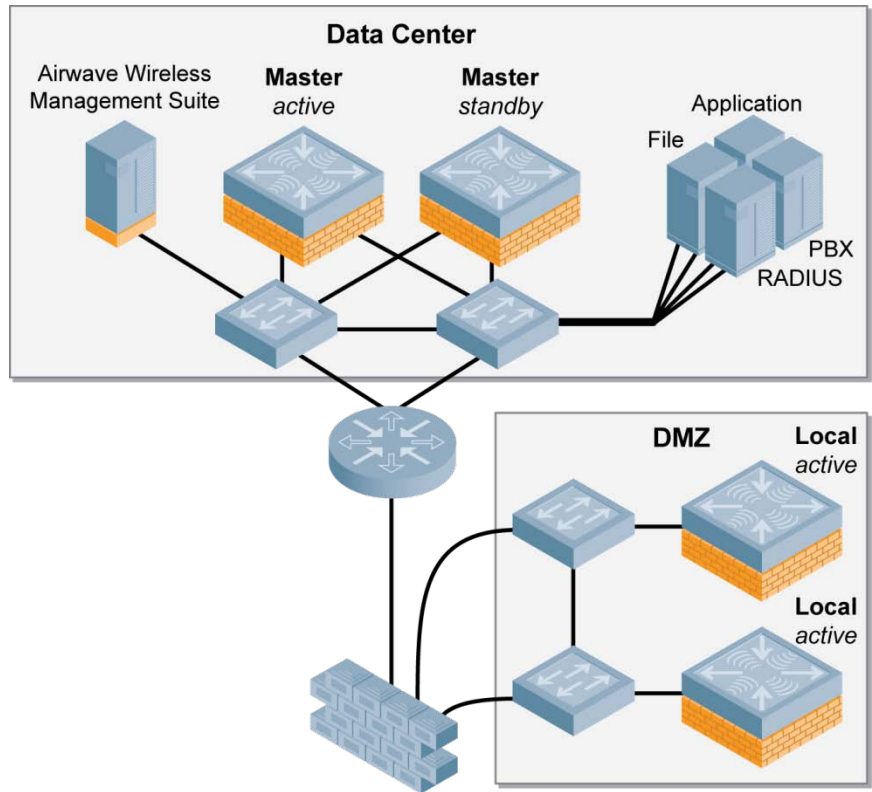
WIPS detects, reports, and mitigates branch office wireless threats such as rogue access points and misconfigured client devices. It also protects against rogue access points by correlating on-air and on-network transmissions, and by watching for known attack signatures. If an attack or vulnerability is detected, the system can alert administrators and provide suggested corrective actions. This feature is especially important for organizations facing PCI (Payment Card Industry) and other compliance requirements that mandate wireless security measures.

Aruba solves the radio manageability problem by leveraging its experience in large-scale enterprise WLAN to simplify branch office wireless deployments through centralized control and management. Aruba also solves the complex problem of RF channel and power setting with Adaptive Radio Management (ARM), which automatically configures wireless settings to minimize interference and maximize performance.

Reducing Complexity through Centralized Configuration, Management, and Troubleshooting

VBN centralizes management of remote systems and, through a common configuration standard, allows all management and troubleshooting to be handled by a single IT group on a single platform. For example, following power-up and connection to the data center controller, a RAP will automatically download its configuration file and software updates over a secure link. This feature eliminates the need to manually update hundreds or thousands of remote devices. Configuration data and software are stored on the Aruba controller in the data center, and are under the control of IT management at all times.

Troubleshooting and reporting can be performed by either the AirWave Management Platform (AMP) or the Aruba controller. AMP provides visibility into the LAN side of the branch office and includes information on both individual users and devices. AMP links into other existing IT management software, provides extensive reporting capabilities, and has specialized views for Help Desk, Security/Audit groups, and executive management.



The Data Center with Airwave Management Platform

Both AMP and the controller allow network engineers to assess the state of devices and connections, as well as perform any required configuration of policy and endpoints. AMP includes many rapid troubleshooting and diagnostic tools that link into Help Desk screens for speedy problem resolution. AMP can also store multiple configuration files to simplify configuration if an organization synchronizes its campus WLAN and branch offices with identical policies.

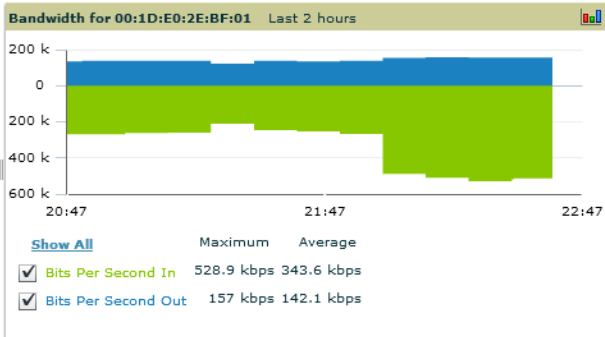
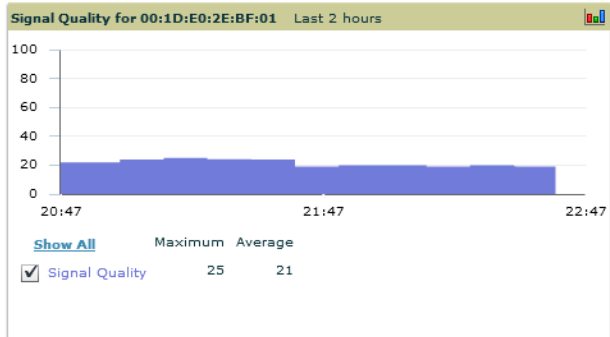
Detail for 00:1D:E0:2E:BF:01

Device Information

Username: -
 Vendor: Intel Corporate
 First Seen: 4/23/2009 1:02 PM on 00:0b:86:c3:5e:27 for 1 hr 5 mins
 Last Seen: 4/28/2009 10:46 PM on 00:0b:86:c3:5e:27 for 3 hrs 16 mins
 Classification: Unclassified

Alert Summary at 4/28/2009 10:46 PM

Type	Last 2 Hours	Last Day	Total	Last Event
AMP Alerts	0	0	0	-
Incidents	0	0	0	-
RADIUS Authentication Issues	0	0	0	-



AMP User Screen

To simplify remote troubleshooting, RAPs feature a diagnostic screen that can be accessed locally by the end user. This feature facilitates remote troubleshooting if a RAP fails to connect to the data center.

RAP Console



SUMMARY Connectivity Diagnostics

Connection Status: Connected Basic [Advanced](#) Last updated: 10:48:43 PM [Refresh](#) [Generate & save support file](#)

Wired Ports	
Port	Status
0 (uplink)	Connected
1	Disabled

Wireless SSIDs		
SSID	Status	Band
rn-demo-employee	Up	2.4GHz
rn-demo-guest	Up	2.4GHz
rn-demo-voice	Up	2.4GHz

Wired User	
Mac Address	IP Address

Wireless User	
MAC Address	IP Address
00:21:5c:50:01:91	172.16.0.231

Device Info	
Type:	RAP-2WG
Name:	00:0b:86:c3:59:e6
Wired MAC address:	00:0b:86:c3:59:e6
Serial #:	AH0000580
Tunnel IP address:	192.168.253.111
Software Version:	ArubaOS Version 3.3.2.11-rn-3.0.0
Up time:	7 min
Master:	63.82.214.195
Ims:	172.16.0.254

Uplink Info	
Port 0 (active)	
Port Speed: 100Mb/s	
IP address: 192.168.1.103	

RAP Console for Remote Troubleshooting

Deploying Aruba's Virtual Branch Network Solution

There are four steps required to successfully deploy Aruba's Virtual Branch Network Solution: (1) implement low cost, zero-touch RAPs and BOCs at the remote sites; (2) leverage commodity transport instead of expensive, private WAN clouds; (3) centralize management and control in the data center using an Aruba controller; and (4) deploy user-centric management with Aruba's AirWave Management Platform to provide visibility into all users and devices in the network.

In the deployment phase Aruba RAPs and BOCs are sent to the remote site with minimal or no preconfiguration to be installed by end users. Aruba RAPs support self-provisioning, while the BOC requires minimal configuration to create a 'plug-and-play' network experience.

During the designing phase consideration needs to be given to what level of WAN connectivity is needed at each remote site. In many instances, commoditized transport links such as business class DSL and cable are sufficient to meet site needs.

The Aruba controller is deployed in the data center, at the front-end the remote network. All RAPs and BOCs connect to this controller, which serves as the system control point and the platform for managing the remote sites.

AMP provides detailed reporting and troubleshooting network-wide, and its detailed statistics, real-time network views, and advanced Help Desk applications make it an indispensable tool for remote networking applications.

Lowering Cost and Complexity of Remote Networking

As the migration to distributed workforces drives up the demand for remote networking, and the quest for expense reduction drives down available funding, the VBN solution stands out as a best-in-class solution for branches of one to many. Aruba's VBN solution features secure one-touch installation by end users, is WAN agnostic and supports low-cost commodity transport, features centralized management and control in the data center, and leverages Aruba's AirWave Management Platform to provide visibility to all users and devices in the network. Taken together these features deliver a powerful, secure branch office solution, at low cost, that consumes minimal IT overhead.

Instead of replicating expensive and complex point products at every site, Aruba has drawn a page from the server virtualization experience to consolidate complex tasks in the data center and virtualize services to low cost edge devices. VBN at last does for branch connectivity and security what data center virtualization did for desktop applications.

Common Remote Applications

The availability of a low-cost, always-on, easily deployable branch office solution makes it economical to deploy remote networking across a wide range of new applications.

The Remote Branch Office

Whether a branch of one or two hundred, users at these facilities typically need access to local resources (such as file servers and printers), both wired and wireless network connections, and in the latter case wireless encryption and intrusion protection to ensure the integrity of enterprise data.

Retail Store Networking

Retail kiosks, stores-within-a-store, and branches need a remote networking solution that can be deployed without IT assistance, offers reliable connectivity for wireless scanners and wired/wireless voice over IP (VoIP) phones, and high security features that address PCI compliance requirements.

The Branch of One – Fixed Telecommuter and Executive Home Office

Fixed telecommuters work from a home office and require access to the same enterprise resources remotely as they would need in the corporate office. User-deployable yet feature rich, RAPs deliver high performance Wi-Fi and secure wired access to wireless laptops, wired VoIP phones and network printers. Aruba's unique policy-based forwarding gives IT managers very wide latitude with respect to local access rights including Internet access.

The Virtual Call Center

Call centers are data and voice intensive applications. Even the least expensive RAP provides a secure means of connecting a VoIP phone and PC to the data center over a consumer DSL or cable connection. VBN is a very affordable solution for even the latest call center deployment, and allows both temporary and full-time users to work efficiently from homes or satellite offices.

Telemedicine

The widespread use of telemedicine hinges on the availability of low-cost, self-installed networks that reliably exchange data without compromising privacy. VBN is a cost-effective solution for securely delivering telemetry, diagnostic, patient record, digital imaging, and other telemedicine applications between a healthcare facility and remote locations.

The Virtual University

As more universities establish virtual campuses and cultivate distantly-located students, the need grows for cost-effective remote access to university resources. VBN is the ideal solution for these applications because low-cost RAPs can economically provide network access to literally every remote student to support wireless PCs, iPhones, and other educational tools. Network integrity is assured, collaboration and innovation enhanced.

Emergency Preparedness and Disaster Recovery

In the event of a natural or manmade disaster or pandemic, VBN provides a simple, effective means by which enterprises can continue to function if workers need to be deployed to their homes or other locations. VBN also allows emergency personnel to be deployed on a wide scale while keeping them in touch with critical emergency resources. 3G cellular support allows RAPs to be deployed with no advanced planning, making VBN also well suited for rapid deployment operations.



1344 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
<http://www.arubanetworks.com>