Enterprise

Virtual Branch Networking (VBN) 2.0 and the Emergence of Cloud-Based Branch Offices
April 2010

ARUBA®

n e t w o r k s

Table of Contents

Virtual Branch Networking (VBN) 2.0 and the Emergence of Cloud-Based Branch Offices

The Challenge

There has been a significant shift during the past 10 years in the way people work, and this has created an extraordinary impact on corporate IT organizations.

The first game-changer was mobility. With mobility, the end user gained the freedom to work anywhere at any time, which increased productivity. In 2009, laptop computers outsold desktop computers for the first time in history.

The workforce then began to disperse. Inroads into new geographic markets created a need for multiple branch offices, while legions of home offices and teleworkers began to grow. IT organizations tasked with delivering enterprise IT services to these remote sites quickly realized that a branch office with one person required the same services as an office of 100 people.

At the same time, servers were consolidated in fewer data centers and applications were outsourced, bringing about virtualization and cloud computing. Applications appeared local to users but were in fact distributed throughout the cloud at geographically dispersed data centers. And workers needed consistent, secure access to these applications, whether at headquarters, branch offices, at home or on the road.

The last significant change has been the availability of affordable, reliable and fast broadband connections. Today, it is possible to obtain a DSL, cable or 3G connection in days or even hours. The widespread availability of broadband made it cost effective to connect a growing number of branch offices, teleworkers, retail stores and home agents to corporate IT resources.

Unfortunately, it is not cost effective to deploy the same IT equipment in small branch and home offices that would be deployed at an office with 100 people. And having to manage that IT equipment across all branch offices – routers, switches, WLANs, local servers and WAN optimization appliances – causes operating costs to skyrocket. As a result, application performance, threat protection and other network services are often sacrificed at small offices.

In an attempt to overcome this challenge, some networking vendors created *branch office-in-a-box* solutions, which consolidated multiple functions into a single product. Although a *branch office-in-a-box* is a less costly alternative to multiple standalone appliances, they are still prohibitively expensive for small branch offices and require IT organizations to create, manage and maintain separate configurations at every single location.

What's needed to create a consistent, high-quality IT experience for small branch offices is a completely new architecture. These offices need a compact, simple, and affordable device that is managed centrally in the data center. Compute-intensive network services like security and application acceleration are pushed into cloud services.

Cloud-based Virtual Branch Networking (VBN) 2.0 From Aruba Networks®

VBN 2.0 from Aruba Networks® delivers the corporate network to small offices with up to 60% capital and 75% operational cost savings compared to traditional branch routers. By migrating network and security services to the cloud, VBN 2.0 replaces costly branch routers with a simple, compact and affordable centrally-managed device called a Remote Access Point (RAP).

Enterprise network services – including user access policies, SSIDs, administration and network monitoring and visibility – are all centrally configured and managed in the corporate data center. Additional cost savings are realized by leveraging broadband connections in branch offices instead of expensive private WAN connections.

The VBN 2.0 architecture encompasses both wired and wireless remote access, with options that scale from very large branch offices all the way to home workers and business travelers. It also integrates seamlessly with centralized administration to reduce operating expenses. With VBN 2.0, application acceleration and content security services are moved into the cloud, which eliminates the need and capital cost for on-site equipment to support these services. And finally, VBN 2.0 ensures a high-quality IT experience for branch office users and gives them secure access to the same resources they would have at corporate headquarters.

The VBN 2.0 Architecture and its Components

The VBN 2.0 architecture has three components. First, Mobility Controllers in the corporate data center virtualize and control the remote network, collapsing branch office functionality to a centralized location where applications are hosted.

Second, Remote Access Points, or RAPs, virtually extend branch office networks from the corporate data center using VPN tunnels. Featuring no-touch deployment, RAPs are easily installed by users at the branch office without IT assistance. Once connected, RAPs provide local wired and wireless connectivity, and localize security and traffic policy enforcement.

Third, the AirWave Management Platform unifies management of all remote access sites and users. The management system performs configuration control, monitoring and troubleshooting functions. Because VBN is an identity-based, policy-driven system, individual accounts, credentials and roles are taken from existing corporate directories, rather than requiring separate configuration.

Figure 1. VBN 2.0 delivers the cloud-based branch office.

A key advantage of the VBN architecture is that, since network functions are centralized and virtualized, RAPs are simple, low-cost plug-and-play devices that allow no-touch branch office deployment. Despite this reduction in complexity, the solution delivers enterprise-class functionality and security.

The cloud-based branch office virtualizes port, VLAN, router, firewall, VPN and quality-of-service (QoS) configurations into a series of identity-driven policies that are centrally defined, and then pushed on-demand to edge devices as users join the network. Resource intensive services such as content security and voice are pushed into the cloud, where economies of scale push down costs. Because these services are moved out of edge devices, the hardware remains viable for a much longer period. Service upgrades are performed in the data center and the cloud, not at every edge device.

The integration of a number of functions into the Mobility Controller is critical for cost-effective performance. By integrating authentication, encryption, firewall and QoS features into a single device, the network administrator has a single point of control for configuration, maintenance and troubleshooting. This reduces initial capital expense and ongoing operating costs. It also provides a solution that does not place any additional burden on the user beyond standard login credentials. Whether at the home office or on-campus, network access procedures are identical.

The Remote Access Point (RAP)

Figure 2. RAPs are simple, compact and affordable to right-size the branch infrastructure.

On network side, the RAP appears like a VPN *client-in-a-box*. Its unique no-touch deployment requires no IT assistance in the branch office. The RAP simply plugs into a branch office network connection, automatically acquires an address and builds an IPSec tunnel to the Mobility Controller in the data center. RAPS exhibit incredible scale and can economically support a home office or a multi-user branch office.

On the LAN side, facing the user, the RAP provides both wired and wireless connectivity options. The integrated RAP delivers full enterprise-class security, management and control using the same technologies as on-campus WLAN deployments. The RAP also provides full wireless security and intrusion prevention (WIPS) services to control rogue access points (APs) and misconfigured clients.

Integrated within the RAP is a policy enforcement firewall (PEF). This is a per-user stateful firewall that acts as an access forwarding engine. It controls connectivity and prioritization based on users and policies rather than ports and subnets to simplify service delivery and security policies to users. The policies applied by the RAP's PEF are set by configuration in the central Mobility Controller based on network-wide templates.
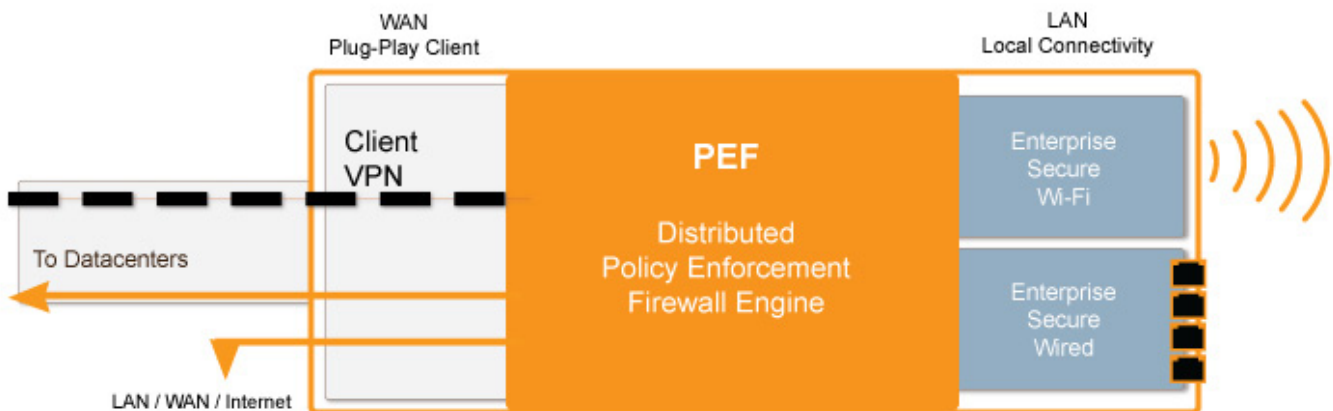

Figure 3. Aruba RAP Functional Diagram.

RAPs can be configured to offload Internet-bound traffic directly to the carrier without transiting the corporate data center. With VBN 2.0, In addition to embracing cloud-based services such as application acceleration, RAPs direct Internet-bound traffic to a content security service in the cloud.

The Mobility Controller

Figure 4. The Aruba 6000 Controller supports up to 8,192 RAPs.

The Mobility Controller includes a fully integrated VPN concentrator to terminate and manage all RAP connections. It also includes a comprehensive centralized WLAN control system. This allows for state-of-the art secure wireless access and wireless intrusion detection system (WIDS) scanning at remote sites but with the real-time centralized control and visibility you get with a local on-campus solution.

Each Mobility Controller's PEF functions as a centralized point of policy definition and as well as a secondary security point for traffic coming into the data center from remote sites.
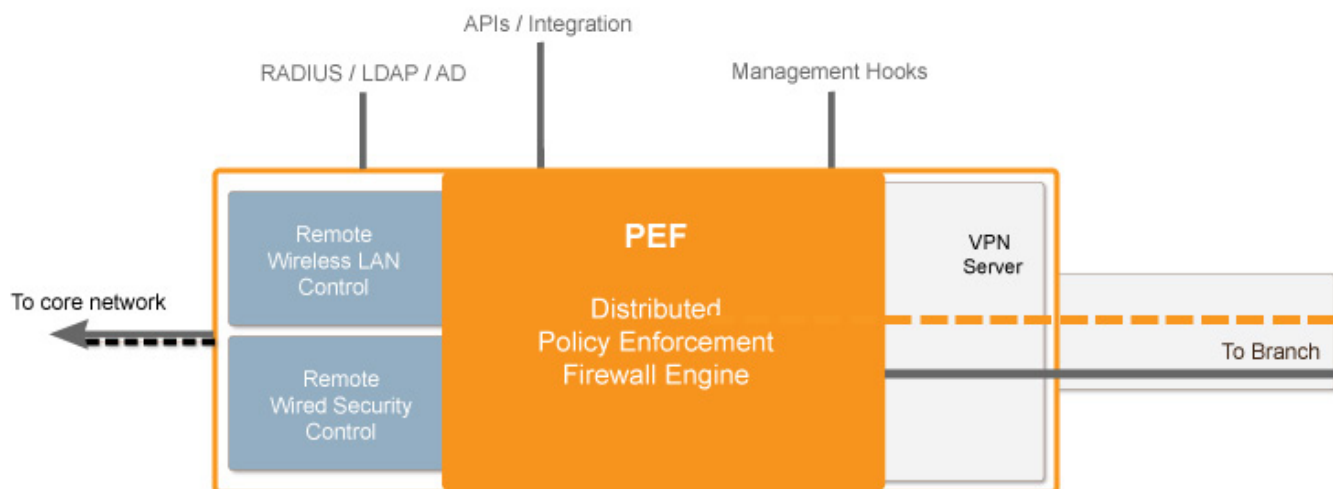

Figure 5. Aruba Mobility Controller functional diagram

Lastly, these systems are built with APIs and integration hooks to tie in with existing public key infrastructure (PKI), management systems and other security systems such as RADIUS for 802.1X access policy enforcement.

A family of Mobility Controllers can scale to support up to many thousands of RAPs and remote devices. The network can include multiple Mobility Controllers that are networked for optimum traffic distribution but managed centrally with uniform policies to enhance operational efficiency.

The AirWave Management Platform

The AirWave Management Platform – part of the AirWave 7™ Wireless Management Suite – is a single pane of glass to manage all remote access in the distributed enterprise network. It manages users and reduces the configuration of a new user to a single-page template for unprecedented simplicity.

Once configurations are complete, AirWave tracks users wherever they access the network and provides vital reporting, auditing and troubleshooting information. Different user views offer troubleshooting tools for the helpdesk as well as escalation engineers.

In addition to users, AirWave manages the entire remote infrastructure. It also has multivendor reach for both wired and wireless equipment to unify the management of legacy APs and switches along with VBN equipment.
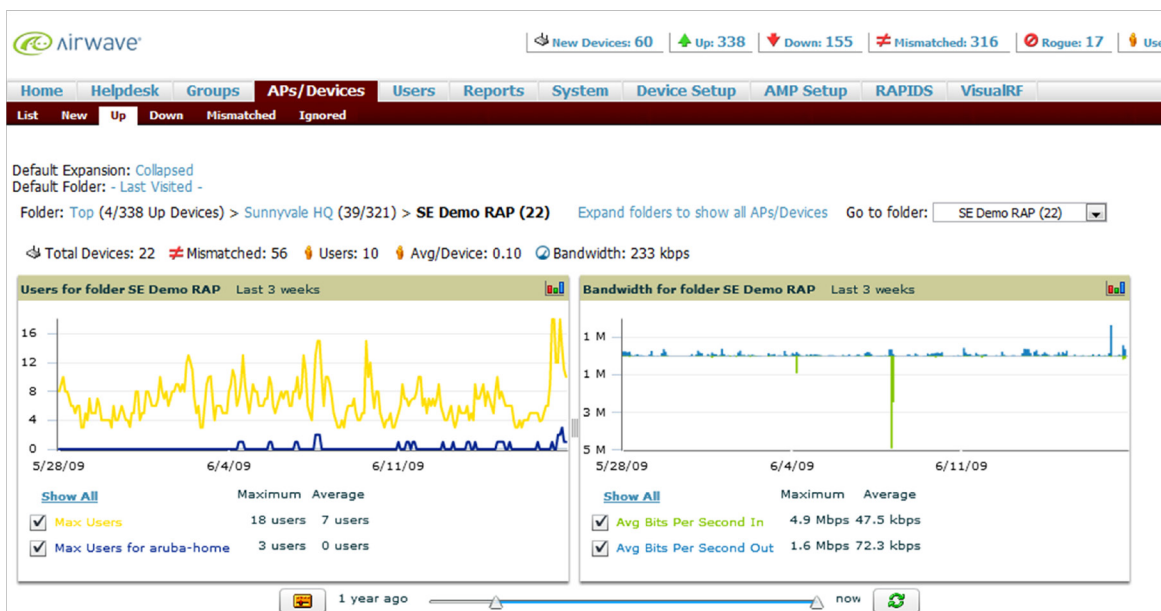

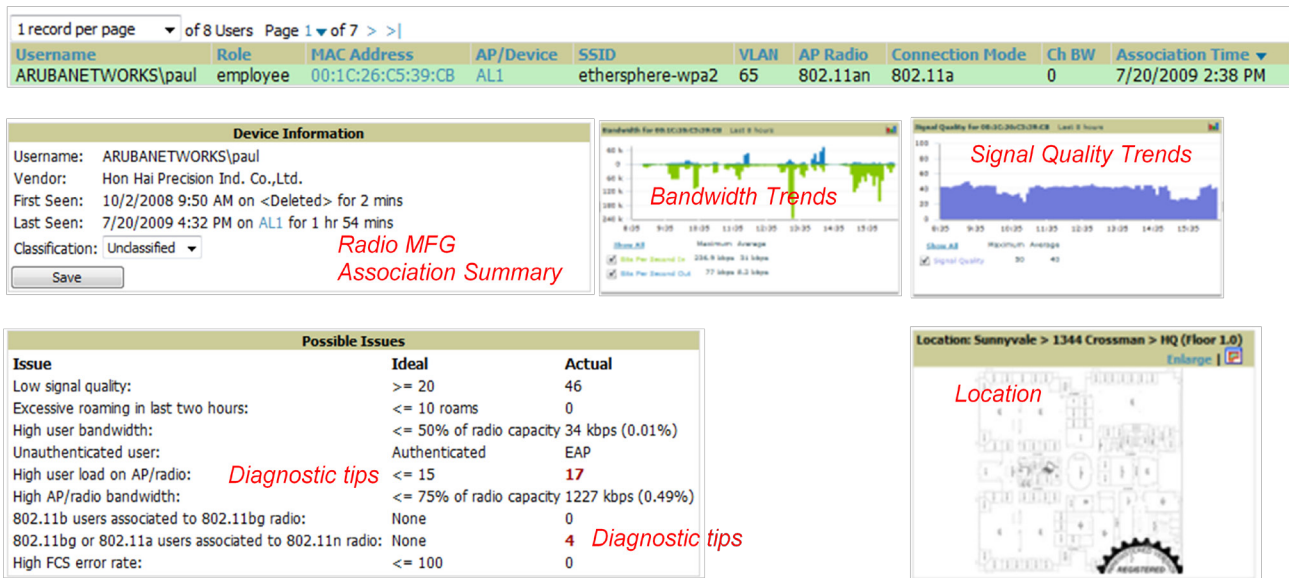*Figure 6. AirWave RAP Monitoring (Partial screen)*

1 record per page	of 8 Users	Page 1 ▾ of 7 > >|							
Username	Role	MAC Address	AP/Device	SSID	VLAN	AP Radio	Connection Mode	Ch BW	Association Time ▾
ARUBANETWORKS\paul	employee	00:1C:26:C5:39:CB	AL1	ethersphere-wpa2	65	802.11an	802.11a	0	7/20/2009 2:38 PM

Figure 7. AirWave User Monitoring (Partial screen)

Application Acceleration Service (AAS)

All employees, including the 88% working outside corporate headquarters sites, demand ever-increasing flows of data to do their jobs. As they become more distant from the data center, the round-trip delays involved in retrieving files and other information from corporate servers start to impede work performance.

It has been common to deploy WAN optimization appliances to overcome these performance challenges. However, this technology requires additional equipment at every remote site or yet another PC clients – which collectively contribute to greater administrative complexity and higher branch office operating costs.

Aruba's cloud-based Application Acceleration Service (AAS) – a pre-eminent feature in VBN 2.0 – accelerates the performance of applications in branch offices without requiring any new hardware or software in the branch. An optional subscription-based file-caching service can further speed up application response times by leveraging a cloud-based content delivery network (CDN) to serve files locally from the nearest data center.

When a remote worker requests a file or other data, AAS automatically matches the request to cached content, and delivers the data from the CDN location closest to the user. This has dual benefits. First, it reduces the round-trip time, and hence accelerates responsiveness and productivity for the user. Second, it reduces the load on the Internet connection at the corporate data center, as each file is transmitted only once from data center to the cloud, where the CDN replicates to all locations.
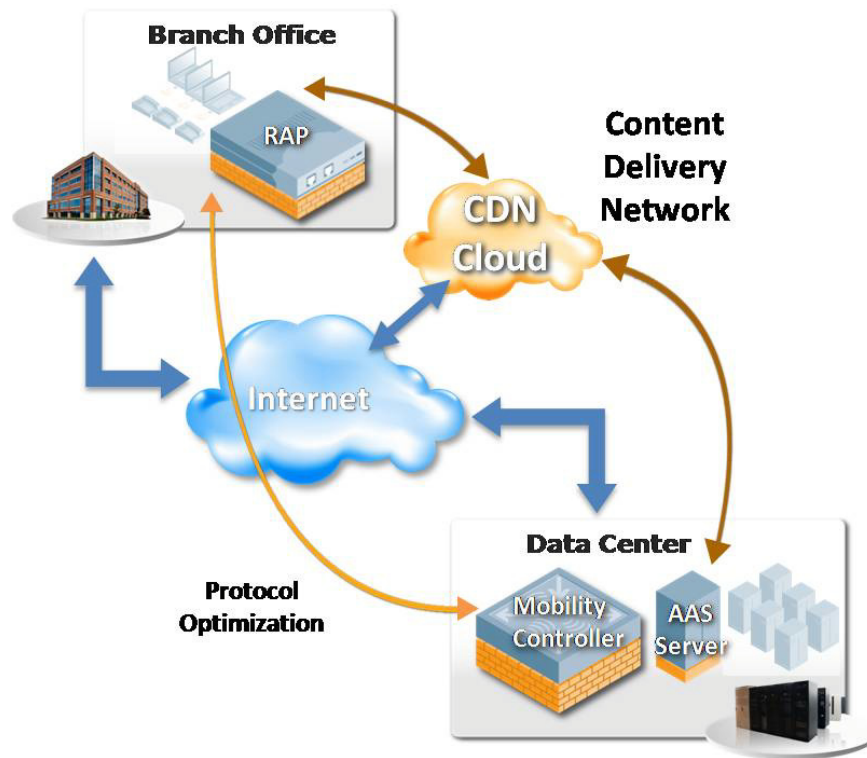
Figure 8. VBN 2.0 Application Acceleration Service (AAS)

In addition to cloud-based CDN replication, AAS implements the widely-known acceleration techniques of compression, keep-alive and protocol spoofing to improve performance of Microsoft SharePoint, Exchange and file sharing at branch offices. To ensure security and information integrity, all data is encrypted using the Advanced Encryption Standard (AES) cryptographic cipher.

Content Security Service (CSS)

Most branch offices and home workers now enjoy short-cut Internet tunnel access through split-tunnel networking. With split-tunnel networking, users can employ a VPN client to securely access corporate network resources and at the same time use a direct Internet connection for general web browsing. This optimizes performance while offloading the corporate WAN pipe.

Although split tunnels are effectively firewalled in the VBN 2.0 architecture to prevent web-to-corporate traffic leakage, connections to the Internet – especially web browsing and Internet-hosted email services – can expose an employee's computer to all manner of malware, trojans and viruses.

On-campus users are often protected by corporate content filtering services, but it is prohibitively expensive to deliver these services locally at small branch offices. An on-site content filtering appliance must be installed or all traffic must be backhauled to the corporate data center for content security screening, which negates the advantages of split-tunnel access.

Aruba's cloud-based Content Security Service (CSS) – another critical feature of VBN 2.0 –

solves this dilemma for branch offices by providing high-throughput, low-latency content security with centralized reporting and management.

Leveraging data centers around the world, CSS provides complete protection including advanced URL filtering, P2P control, anti-virus, anti-malware, botnet detection and data loss prevention (DLP). High-speed web logs in CSS provide a flexible and powerful way to view both broad trends and per-user drill downs of Internet activity.

Figure 9. VBN 2.0 Content Security Service (CSS)

Operational Overview of the VBN 2.0 Solution

Remote Access Networking with VBN 2.0

The RAP is designed to be shipped to remote sites in the original unopened package for installation by non-technical employees. Its no-touch deployment approach means no IT intervention is required at the remote site. The installation process is extremely simple: Connect the RAP to a WAN or Internet router in the branch or home office, plug a PC into the RAP's Ethernet port and connect the power cable.

The user is then directed to enter the Internet address of the corporate Mobility Controller. When this is done, the RAP automatically discovers the Mobility Controller, authenticates and sets up an IPSec tunnel for control traffic. No further action is required at the site. All configuration information is downloaded via the central site.

Forwarding and Operating Modes: Centralized Traffic, Local Bridging and Split Tunnels

Full-tunnel SSID traffic on a RAP is destined for the corporate data center, and this is encrypted end-to-end using AES and backhauled from the RAP via IPSec encapsulation.

However, many branch offices and even some home offices have a number of local servers, printers and other devices they may wish to network via the RAP. Instead of backhauling this traffic to the data center and hair-pinning the return path – which introduces delays and consumes WAN bandwidth – VBN 2.0 allows this traffic to be bridged locally.
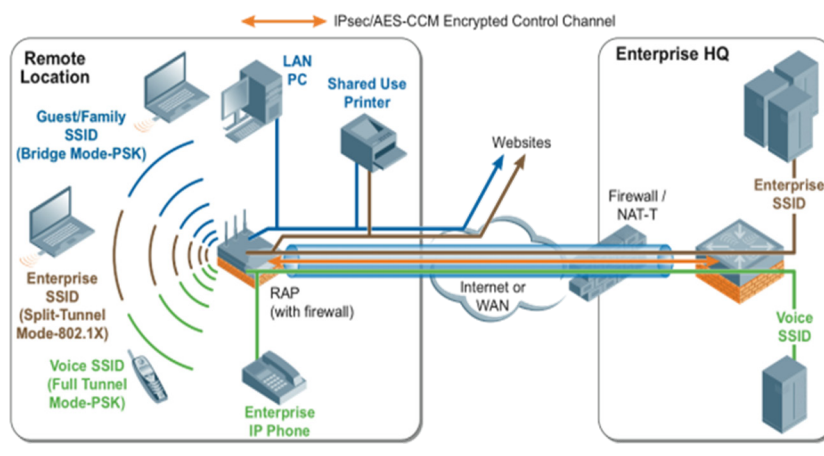

Figure 10. VBN Forwarding and Operating Modes

Split-tunneling is handled directly at the RAP to offload the corporate data center and improve performance. As mentioned previously, split tunneling can potentially leave users vulnerable to malware, trojans and viruses on the Internet link. To prevent this from happening, the RAP incorporates a stateful firewall and can direct Internet-bound traffic to the cloud-based content security service for deep packet inspection.

Centralized and Local Encryption Options

VBN 2.0 utilizes the military-grade AES used in the Wi-Fi WPA2-enterprise protocol. This is a complex cryptographic cipher and requires considerable processing, but it remains the toughest security standard for Wi-Fi connections. VBN 2.0 incorporates AES in hardware to ease the load on the RAP main processor.

Because AES-capable hardware is built into all common devices and represents the highest level of protection, it makes sense to use this as the pervasive encryption method for data between remote clients and the corporate data center. In the VBN 2.0 architecture, all user data is AES-encrypted from end-to-end using individual keys. A GRE header is added to facilitate tunneling to Mobility Controllers over the Internet or corporate WAN. Control traffic for the RAP has its own independently-secured IPSec tunnel.

While this is an optimum configuration for data center-bound traffic, the VBN 2.0 architecture supports other flexible network routing options when traffic does not terminate at the data center. In this case, AES is still employed over the air, but decryption takes place on the RAP rather than at the central Mobility Controller.

WLAN Functionality for Remote Access

Wi-Fi introduces unique networking scenarios that cannot be experienced in wired infrastructures. For example, frames passing over the air are subject to errors due to radio frequency (RF) interference and signal strength fluctuations. To minimize this, Aruba's Adaptive Radio Management (ARM) system provides tools to visualize and automatically optimize RF coverage. Whether in the branch office or on campus, ARM automatically chooses the optimal RF settings for the RAP, continually monitors the air for signs of interference and switches to alternate channels when appropriate.

Wi-Fi clients are typically configured with a list of acceptable SSIDs, and periodically wake the Wi-Fi radio and probe for these SSIDs. When setting up client devices for use in VBN 2.0 environments, simply configure the corporate SSID at the top of the list – the same SSID that is used on-campus. Authentication with this SSID is typically handled through a login method, such as Windows login, and leverages 802.1X authentication and corporate RADIUS servers.

On the network side, RAPs offer the same services and are configured with the same templates as on-campus APs. Its SSID offers an extension of the corporate network to the branch or home office no matter where they are located.

From the user's viewpoint, a uniform corporate SSID for on-campus and remote access requires only one login procedure. There is nothing additional to remember, no workflow change and security is completely transparent, which reduces IT costs and helpdesk calls. Furthermore, centralized troubleshooting brings down the operational costs of the VBN 2.0 solution.

Assuring Multimedia Performance with QoS

As voice-over-WLAN and Fixed Mobile Convergence (FMC) solutions become more common, QoS becomes critical to control multimedia traffic streams that are generated and terminated in the branch or home office.

The RAP and Mobility Controller are able to identify and correctly prioritize multimedia traffic, even though it does not always arrive over the Internet or from client devices with priority tags intact. This is accomplished using firewall rules that identify streams and re-apply appropriate tags.

Over-the-air QoS is affected by the wireless multimedia (WMM) protocol now available on all Wi-Fi devices. WMM ensures that multimedia traffic is promptly delivered even when the network is overloaded with data. It specifies mapping to differentiated-services code points (DSCP) and IP type-of-service (IP TOS) tags to maintain end-to-end priority.

Since smartphones and other converged devices generate voice and data over a single connection, it is no longer possible to separate each traffic type with separate SSIDs and underlying VLANs. VBN 2.0 does not require such configurations.

Other QoS provisions supported by VBN 2.0 include call admissions control (CAC), which ensures that the number of voice and video calls allowed does not exceed the network or backhaul capacity. VBN 2.0 also supports a flexible policy-based bandwidth manager for fine-grained traffic control capabilities in multi-tenant networks and during periods of network congestion.

Security in a VBN 2.0 Network

In addition to the comprehensive threat detection and prevention capabilities available with Aruba's cloud-based CSS – advanced URL filtering, P2P control, anti-virus, anti-malware, botnet detection and data loss prevention – VBN 2.0 offers a wide range of additional security features. With VBN 2.0, the branch office RAP becomes a secure extension of the corporate network. Configuration control, user access and firewall configurations are all driven by IT from the corporate data center. The result is a fully integrated secure mobility solution that maintains total control over the user experience.

Because VBN 2.0 extends services from the corporate data center to branch offices using the same architecture as campus WLANs, it leverages authentication and encryption methods that are already used by Wi-Fi clients. As the RAP begins operation, corporate client devices see the same beacons and prompts they would see on campus. The user experience is uniform throughout the enterprise, which employs consistent login procedures, authentication with 802.1X and AES encryption.

Meanwhile, VBN 2.0 constantly monitors the wireless environment for intrusion attempts. Wireless represents a security challenge because signals extend beyond the immediate area, allowing monitoring and intrusion opportunities without physical access to the premises.

While scanning the air, RAPs can recognize common attacks and take action against perpetrators. Man-in-the-middle attacks and AP spoofing are detected and contained. Additional information is made available to administrators through integration with traditional WIDS and WIPS and alerts can be generated as countermeasures are launched.

Remote Site Survivability

The most frequent cause of outages in branch offices is failure of the local Internet or WAN connection. A single fault can isolate the branch office and cut off mission-critical services. A traditional workaround solution has entailed provisioning redundant Internet connections, but this increases costs and an outage can still take down both paths. It is very difficult to find truly diverse links at most locations.

Because it is rare for a fault to brown down both wired and cellular connections, VBN 2.0 leverages the cellular data network as an alternate backhaul path. A USB port on the RAP allows the customer to select the carrier of choice by inserting an appropriate data modem device. Cellular connections offer good diversity and are cost effective because the connection is in

backup mode most of the time. Many VBN 2.0 customers already use the cellular data network as the only backhaul connection for a RAP, with good results.

Larger branch offices may have significant intra-branch traffic patterns, and in the event of a WAN outage a RAP configured for bridge mode will maintain this connectivity. Also, if an outage affects the data center, the RAP can continue to offer an Internet-bound split tunnel even though corporate traffic will be blocked.

Scalability

When designing remote access networks with today's technology, it is impossible to apply a single, seamless architecture. Business travelers and home office workers commonly use software VPN clients, while small branch offices tend to use *VPN-in-a-box* appliances from different vendors that require different configuration and management systems. Special demands, such as Wi-Fi and application acceleration, are often met using extra equipment, which increases the cost and complexity of configuration and support.

The difficulties become more evident as branch offices expand. Larger branches require more redundancy, alternative access links for survivability and encompass more people and more services. At some level of scale, the network design must switch again to become a bundle of equipment, replicating the campus site on a smaller scale.

The VBN 2.0 architecture offers a smooth progression – from the business traveler to the large branch office – using the same architecture, unified data center equipment, and a single configuration and management platform. Business travelers can be equipped with an Aruba Virtual Intranet Access (VIA) agent if they need access from public Wi-Fi networks. The RAP-2 is ideal for basic secure Wi-Fi access for home workers. The RAP-5 is ideal for executives working from home, small branch offices and larger branch offices with wired clients such as desk phones or printers.

As branch offices grow and employees require additional services like local servers and printers, it becomes important to provide a higher level of survivability. In this scenario, Aruba's 600 series Branch Office Controllers offer superb resiliency and redundancy along with higher capacity. They autonomously maintain services in the event of WAN failure, but in normal operation they work as subordinates to the data center Mobility Controller. The 600 series Branch Office Controllers are configured using the same interfaces and according to the same architectural principles as other VBN 2.0 equipment.

Conclusion

Branch office networking started with a simple "replicate everything" model – taking all the networking equipment in the corporate headquarters network and bundling smaller versions in branch offices. Every branch was a miniature version of the headquarters site. But this required many complex appliances, multiple management systems, and a frequent need to replace branch office equipment as networking requirements changed.

The amount of equipment was reduced when *branch office-in-a-box* solutions combined routing, switching, VPN, firewall, voice and other security services into a single appliance. This helped reduce footprint and wiring mistakes, but internally these appliances were still multiple independent systems, configured and managed separately.

The Aruba VBN 2.0 architecture *right-sizes* the cost of networking in small branch and home offices by eliminating the need for prohibitively expensive appliances. Instead, enterprise-class services can be securely accessed from branch offices simply by plugging a RAP into a broadband connection. This no-touch deployment approach means no IT intervention is required. The result is a significant reduction in hardware footprint, lower operating expenses, and unparalleled scale without compromising security.

VBN 2.0 migrates compute-intensive services like content security and application acceleration into the cloud, where economies of scale push down costs. By moving these services out of edge devices and into a data center across the cloud, performance is able to cost-effectively scale over a longer period of time. Services upgrades are done in the cloud instead of at every edge device.

The cloud-based VBN 2.0 architecture virtualizes port, VLAN, router, firewall and VPN configurations into a series of identity-driven policies that are centrally defined, and then pushed on-demand to remote edge devices as users join the network. A single, centralized management system controls all user and equipment configuration and policies.

About Aruba Networks, Inc.

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services – regardless of the user's device, location, or network. This dramatically improves productivity and lowers capital and operational costs.

Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter, Facebook, or the Green Island News Blog.

ARUBA
n e t w o r k s

1344 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. 408.227.4500 | Fax. 408.227.4550 | info@arubanetworks.com
http://www.arubanetworks.com

SG_VBN_Cloud-Based_Svcs_100412