Whitepaper |

Enterprise

# The Convergence of Enterprise Telecom Services:

## BlackBerry Mobile Voice System on the Aruba Networks Wireless LAN Infrastructure

## April 2010

Peter Thornycroft

ARUBA® networks

# Table of Contents

## 1.1 Introduction

Modern enterprises are becoming more widely distributed, and workers are increasingly mobile. Fewer employees are working in large corporate offices, with estimates of the remote workforce as high as 80% of employees in some companies[1]. As enterprises hire employees and contractors from a global talent pool, wherever they may live, they are forming virtual teams: the remote worker has become the rule rather than the exception.

Even within ***office*** environments, a recent survey of CIOs[2] estimates that more than 40% of employees' phone calls are already made on cellular phones, and research firm Gartner predicts[3] that by 2013, 40% of knowledge workers worldwide will have abandoned their desk phone. Bridging the gulf between the corporate PBX-based communication system and the cell phone network is an increasingly urgent goal for all enterprises.

As the virtual workforce expands, research in the field reveals that communications is a key factor in maximizing productivity: the most productive remote employees can communicate with colleagues with one click, and have easy access to all IT services available on-campus at the main office. Successful remote workers develop intimate working relationships with their teams, but this is a difficult goal to achieve when remote workers are outside the corporate firewall and face communications barriers when working with colleagues and corporate data applications.

IT groups face challenges in improving this level of communications: the typical remote worker primarily uses a cell phone, and to date cell phones have not been well-integrated with corporate communications systems. While lack of integration presents a productivity barrier for the user, it is also of concern to many organizations where audit trails are required for employees' transactions, as cell phone usage cannot be monitored in sufficient detail. Further, cellular network costs now represent the largest item in many enterprises' telecom budgets, and it has proven extremely difficult to keep these costs in check.

Two new technologies show promise in overcoming these barriers to productivity, cost control and compliance. The first is unified communications (UC), which in its UC-client form provides PBX-like features for cell phones, giving users a seamless and consistent view of corporate communications services based on a single device. A UC-equipped cell phone rings and dials as a corporate extension, with all the short-dialing, presence, directory, call-transfer and other functions expected of a PBX desk phone. It is also a platform for new features such as corporate video calling and corporate social media. For the IT group, the client is managed from the data center, and all transactions can be monitored centrally.

Secondly, fixed-mobile convergence (FMC) has come to the fore in recent years. Here, we define FMC as enabling seamless communications over both the cellular network and Wi-Fi, in this case the corporate wireless LAN (WLAN). Moving communications from cellular networks to the WLAN increases productivity because it provides fully-authenticated and encrypted inside-the-firewall access to all corporate voice and data services. New Virtual Branch Networking (VBN) technology enables inexpensive, user-installable VBN access points (APs) to extend the corporate WLAN across the range of branch offices and home offices. Since transactions on the WLAN are offloaded from the cellular network, application performance is increased while the cellular budget is reduced.

The combination of FMC/UC offers significant benefits for both remote and mobile employees, and for the corporate IT group. When well-implemented, it can deliver seamless, one-touch communications tools wherever the employee wishes to work.

### 1.2 Benefits of FMC/UC

There are three main drivers for FMC/UC. The first is productivity. Providing the cell phone user with an equivalent set of visibility, features and connectivity as a desk phone – and more – enables modes of communication that are not otherwise possible. One significant feature is single-number identity, where an employee can publish one number rather than separate office and cell options. This number is consistently used as the outgoing caller's number, so contact lists can be automatically populated. A single number means fewer calls go unanswered, and those that do will hit the sole (corporate) voicemail box.

Productivity is also improved when remote users are provided with inside-the-firewall features, which enables them to use IM/chat with colleagues and click-to-dial. Indeed, UC vendors are quickly integrating social networking functionality, and FMC/UC deployments offer a useful platform to extend the networking effect of this software to embrace remote employees as well as on-campus use.

Yet another aspect of productivity is that Wi-Fi connections run at higher speeds than the cellular data network. Already, many consumers use the Wi-Fi option on their smartphones, typically at home and in hotspot coverage, because of the better performance. Further, because corporate WLANs provide corporate authentication and encryption, they avoid the need for VPN security, with its extra layers of configuration and processing that impact performance.

The second benefit of FMC/UC is providing coverage where cellular networks are sparse. Many employees find poor cellular coverage in their office, at home, or other places they would like to work. When the same features are available over the corporate WLAN, access points can be self-installed wherever there is a need for coverage, filling the gaps and extending the distributed enterprise network to every employee's office.

The third benefit is in cost savings. The most significant areas where cellular calling costs are reduced with FMC/UC are international calling and roaming. When calling out, even from cellular, it is the corporate IP-PBX that places the international call, so least-cost routing and centrally-negotiated tariffs are used. Alternatively, a user who is traveling internationally can connect over Wi-Fi rather than cellular, avoiding roaming charges. Further savings result from WLAN calls offloading the cellular network, so fewer minutes/month are billed. Because many cellular calls are made from corporate offices, this can represent a high percentage of monthly minutes, although it can take some administrative effort to compile data and negotiate with carriers for new cellular contracts reflecting the lower activity.

### 1.3 Enterprise-centric FMC

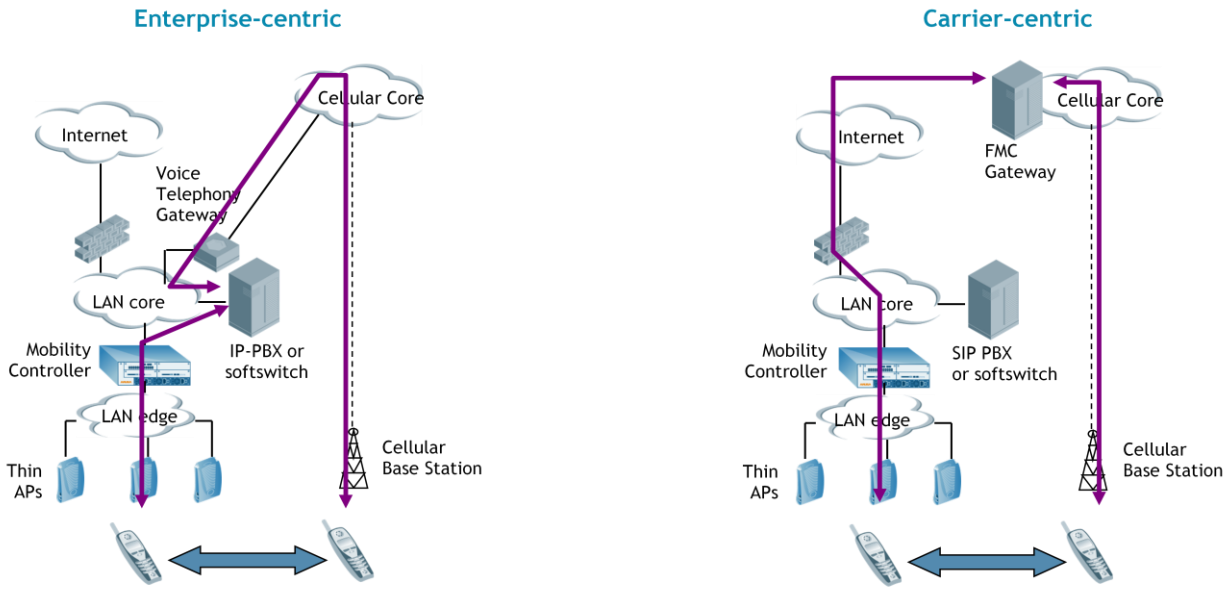



Figure 1. Enterprise-centric and carrier-centric FMC architectures

FMC can be implemented as two architectural models, carrier-centric or enterprise-centric. In an enterprise-centric network, the corporate IP-PBX is the anchor-point for calls, and an FMC call server is inserted adjacent to it. All incoming calls are dialed to the user's direct inward dial (DID) number and all outgoing calls are originated from the IP-PBX, so the "caller-ID" seen by the recipient is the IP-PBX number.

When a phone is authenticated on the corporate WLAN, VoIP protocols connect it directly to the IP-PBX, like a desk phone, and custom software on the phone allows it to emulate feature keys like the desk phone. When outside Wi-Fi coverage, the phone continues to act as a client of the IP-PBX. An incoming call to the IP-PBX DID number is forwarded to the phone's cellular number for completion. When an outgoing call is launched from the phone, it calls back to the IP-PBX (or vice versa) which simultaneously dials a new call leg to the destination. While in communication with the FMC server and IP-PBX, either over cellular or Wi-Fi networks, the phone provides many of the features of a desk phone.

All IP-PBX and UC vendors offer UC-client solutions where employees in cellular coverage can communicate using IP-IP-PBX features in real-time, with capabilities such as integrated presence, short-dialing, corporate directory and instant messaging. To date, few of these vendors have ventured into WLAN connectivity and FMC, but as a Wi-Fi interface is now present on most smartphones, this will become the next level of functionality.

An enterprise-centric architecture is likely to appeal to organizations where there is a strong IP-PBX solution in place. It allows for the extension of useful IP-PBX features as the user roams, whether in Wi-Fi or mobile coverage.

### 1.4 Carrier-centric FMC

While the solution above is focused on equipment installed on an enterprise's premises and integrated with an existing IP-PBX, cellular operators have followed a different path to FMC. They have focused on delivering a richer set of carrier-provided services, delivered over both cellular and Wi-Fi networks. The control point is the operator's core network rather than the IP-PBX. This approach allows consumers to compensate for poor in-home or workplace cellular coverage by installing a Wi-Fi AP, and depending on the tariff, to save money on calls made when in Wi-Fi coverage.

IP-PBXs are not involved in a carrier centric architecture: the handset behaves as a standard mobile phone everywhere, and the subscriber continues to receive the same set of mobile services whether in cellular or Wi-Fi coverage. The cellular number is the 'single number' used for all calls, but the cellular network delivers calls over Wi-Fi and the Internet when the phone is registered via an access point.

With the current trend of offloading cellular data traffic to Wi-Fi, carriers are implementing a number of standards for FMC, including I-WLAN, UMA and VCC. All of these are 3GPP standards, and UMA is already in service with many GSM operators worldwide. While many enterprises are PBX-centric in their voice communications, and will prefer enterprise-centric solutions, carrier-centric FMC will appeal to others, such as smaller organizations which cannot justify dedicated telecom managers.

## 1.5 The BlackBerry® Mobile Voice System

The BlackBerry Mobile Voice System (BlackBerry MVS) from Research In Motion (RIM) is an enterprise-centric FMC/UC solution built around the popular BlackBerry smartphone. It uses software integrated with the native phone application, and the BlackBerry MVS Server hosted by the enterprise, an adjunct to the BlackBerry® Enterprise Server, integrated with the corporate IP-PBX.

The BlackBerry MVS architecture is already used in conjunction with UMA solutions to deliver IP-PBX features from a carrier-centric FMC architecture. The rest of this paper will focus on the enterprise-centric solution and related benefits. Enterprises will be drawn to the BlackBerry MVS enterprise solution for all the productivity, coverage and cost benefits mentioned above, but RIM brings some particular advantages to FMC/UC.

The BlackBerry smartphone is purpose-built for business use, engineered for maximum user productivity, while offering the highest levels of data and communications security. With the BlackBerry Mobile Voice System, RIM has continued this focus. For example by ensuring that all voice signaling is encrypted, it is not possible for an intruder to identify calling/called numbers, or to hijack corporate voice services by impersonating a BlackBerry.

Similarly, the tightly-controlled software environment on the smartphone is utilized to make it possible that all calls made to or from the device are routed via the corporate IP-PBX, and can be logged and recorded. This is an important function for many financial institutions, when an audit trail of calls is required to verify transactions.

Because most large enterprises already use BlackBerry smartphones and the BlackBerry Enterprise Server, they are conversant with the software used to configure these systems, and adding BlackBerry MVS utilizes an existing vendor and familiar look-and-feel. Central management and configuration control for smartphones such as the BlackBerry smartphone is a requirement for large-scale corporate adoption.

User acceptance is a requirement for any FMC/UC solution. The BlackBerry smartphone is designed first and foremost as a business tool. Many knowledge workers would not accept any substitute and they will welcome new capabilities

on their tried-and-trusted device. BlackBerry MVS adds enterprise voice integration to the email and data services integration already offered on the BlackBerry smartphone.

The choice of WLAN for use with BlackBerry MVS is critical to the performance of the overall solution. When on-campus and in larger offices, the WLAN is intimately involved in delivering continuous coverage, enabling inter-AP handovers, maintaining quality of service (QoS) and optimizing battery life. Aruba Networks has a wealth of experience in delivering WLANs optimized for secure multimedia services, and counts the largest and most forward-looking enterprises among its customer list.

Meanwhile, the further the corporate WLAN can extend, the more employees will enjoy inside-the-firewall access to corporate voice and data services. Aruba has pioneered the VBN architecture, where cost-effective, user-installed access points allow branch offices and home workers to enjoy the same level of access as on-campus employees.

### 1.6 The BlackBerry MVS architecture

This section deals with the overall architecture of the BlackBerry MVS solution, the interfaces and protocols used, signaling and call paths and options. It also identifies how calls traverse the enterprise WLAN, and establishes the security architecture.

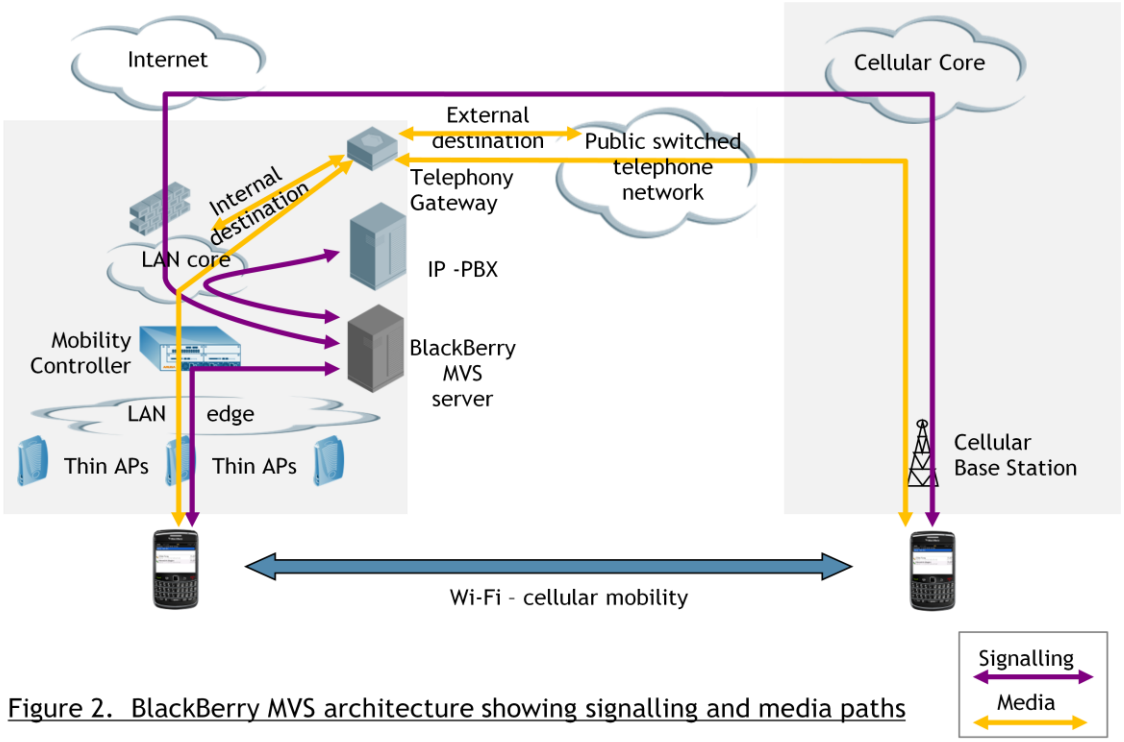



Figure 2. BlackBerry MVS architecture showing signalling and media paths

BlackBerry MVS is an enterprise-centric, IP-PBX-adjunct architecture. The BlackBerry MVS Server works in conjunction with the corporate IP-PBX to route calls to and from the BlackBerry MVS Client. This ensures that all calls are anchored in the enterprise network, enabling single-number capability and switching of calls between cellular and Wi-Fi networks, as well as to IP-PBX extension phones.

The call paths above correspond to the enterprise-centric FMC/UC architecture described earlier, in that the IP-PBX DID number is the 'single-number identity' used for all incoming calls: calls to that number will reach the smartphone whether it is in cellular or Wi-Fi coverage, while outgoing calls from the smartphone are all routed via the corporate IP-PBX and carry the same 'single-number' as the calling number identity.

### 1.7 Call architecture with cellular coverage

Whether in cellular or Wi-Fi coverage, the BlackBerry smartphone maintains a data link to the BlackBerry MVS Server for call features, control and signaling purposes. When the smartphone is in cellular coverage, the appropriate cellular data channel is used by the control link. Since the link is between two RIM-designed entities, it uses a compressed, encrypted proprietary protocol for optimum security and the lowest cellular data utilization. The principles behind this are the same as for the familiar BlackBerry email service.

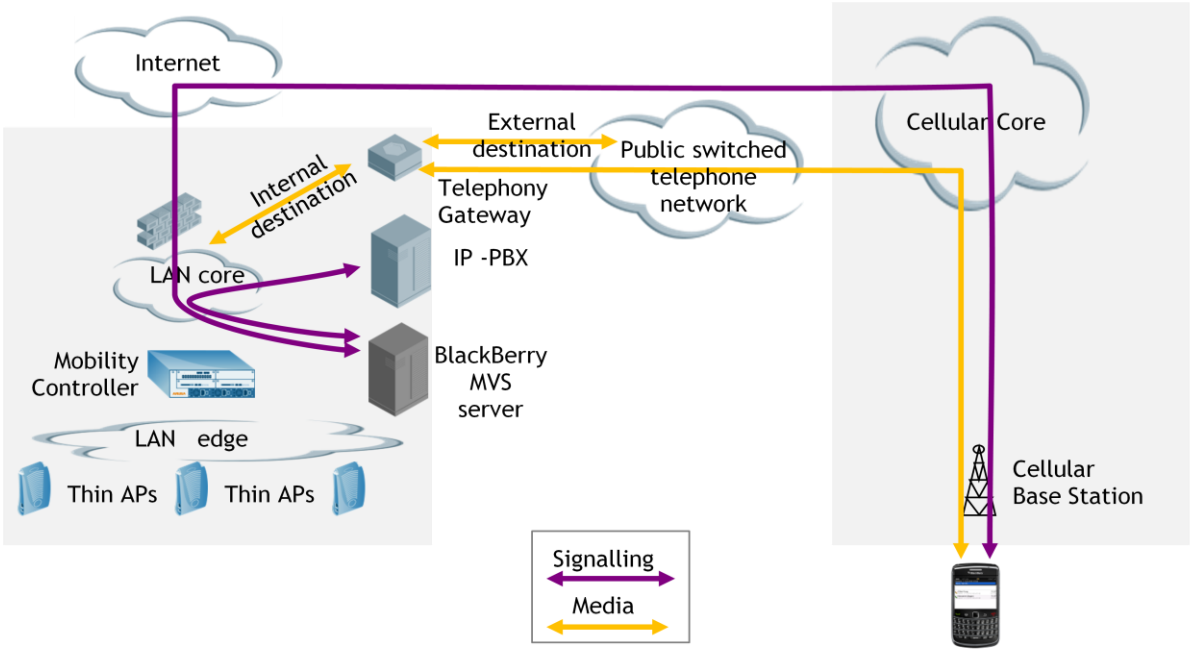



Figure 3. BlackBerry MVS architecture showing signalling and media paths in cellular coverage

For integration with the IP-PBX, the BlackBerry MVS Server uses the SIP protocol. On the IP-PBX side this is configured as a SIP end point per client, and the Blackberry MVS Server acts as a proxy for the BlackBerry MVS Client on the smartphone. Thus the BlackBerry MVS Server converts the compressed signaling used on the MVS link to 'standard' SIP used to communicate with the PBX. Each supported smartphone has an extension configured respectively on the BlackBerry MVS Server and the IP-PBX.

When an employee wishes to make an outgoing call, the BlackBerry MVS Client on the smartphone offers two options. One uses the cellular line configured on the smartphone to bypass the BlackBerry MVS Server and dial directly into the cellular network. The calling number is the cellular line of the smartphone and there is no IP-PBX interaction.

The second mode will be more popular and functional, as it makes use of the BlackBerry MVS features. The BlackBerry MVS Client on the smartphone intercepts the dialed digits and sends them on the communications link to the BlackBerry MVS Server. The server controls the setup of two calls – one between the BlackBerry smartphone and the IP-PBX and the other from the IP-PBX to the required destination.

The call between the smartphone and the IP-PBX is set up first. The system can be configured to originate the call from the IP-PBX or from the smartphone. Either option may be advantageous for cost control or other reasons, depending on the environment.

Once the call leg between IP-PBX and smartphone is complete, the second call is originated from the IP-PBX, under control of the BlackBerry MVS Sever, to the original destination dialed by the smartphone user. Both call legs will use the IP-PBX's least-cost routing and call-restriction capabilities, if they are originated at that end. After both calls are completed, the BlackBerry MVS Server instructs the IP-PBX to bridge them together and the smartphone user can converse with the destination.

Incoming calls to the phone use the corporate DID number or corporate extension which is the single number identity. Because the BlackBerry MVS Server is a SIP proxy for the smartphone, it is notified of the incoming call by the IP-PBX and immediately initiates an outgoing call to the cellular number of the smartphone. The caller's information, such as the calling name or number, is sent on the data channel to the smartphone, to ensure that it arrives in advance of the call. When the smartphone answers, the calls are bridged by the IP-PBX under control of the BlackBerry MVS Server.

While the signaling path always includes the BlackBerry MVS Server, the media stream is anchored on the corporate telephony gateway under immediate control of the IP-PBX, while third-party call control is handled from the BlackBerry MVS Server.

When the BlackBerry smartphone calls a corporate extension rather than a PSTN destination, the BlackBerry MVS Server processes the call in the usual way and the IP-PBX recognizes it as an extension and routes appropriately.

### 1.8 Call architecture with WLAN coverage

When the BlackBerry smartphone is connected over the WLAN, it uses the same signaling and control protocol carried over cellular data to communicate with its BlackBerry MVS Server. As noted before, this is a proprietary protocol, compressed and encrypted.

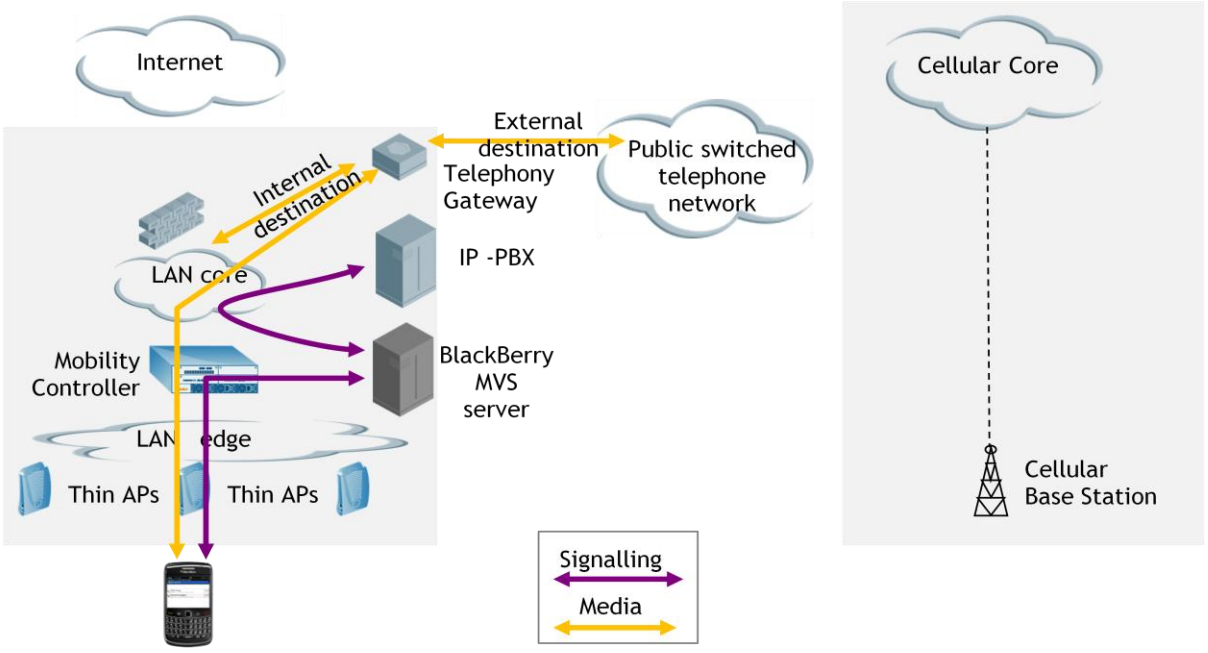



Figure 4. BlackBerry MVS architecture showing signalling and media paths in Wi-Fi coverage

Outgoing calls to external numbers are originated by dialing at the smartphone, with the digits sent to the BlackBerry MVS Server. The BlackBerry MVS Server acts as a SIP proxy for the smartphone, initiating an outgoing call through the

IP-PBX. There is only one external call leg in this model, rather than the two legs required when the smartphone is in cellular coverage.

Similarly, for incoming calls the IP-PBX sees an incoming DID call and directs it to the BlackBerry MVS Server as a SIP proxy for the BlackBerry MVS Client.

When the smartphone is in Wi-Fi coverage at a hotspot or domestic access point, it can connect over Wi-Fi and communicate with the BlackBerry MVS Server, routing calls in the same way as described above.

### 1.9 Moving calls between networks

All the call models shown above involve the BlackBerry MVS Server as the anchor point in the signaling path, with the corporate telephony gateway anchoring the media stream. These anchor points are required to move calls between networks because a cellular-to-cellular call would not otherwise touch the IP-PBX and therefore could not be moved to Wi-Fi. The BlackBerry MVS solution supports several types of call transfer or movement, all initiated manually.

- Move to/from Wi-Fi
- Move to desk phone
- Move to arbitrary number

All of these are accomplished using the control link to the BlackBerry MVS Server, with the server using third-party call control through the IP-PBX.

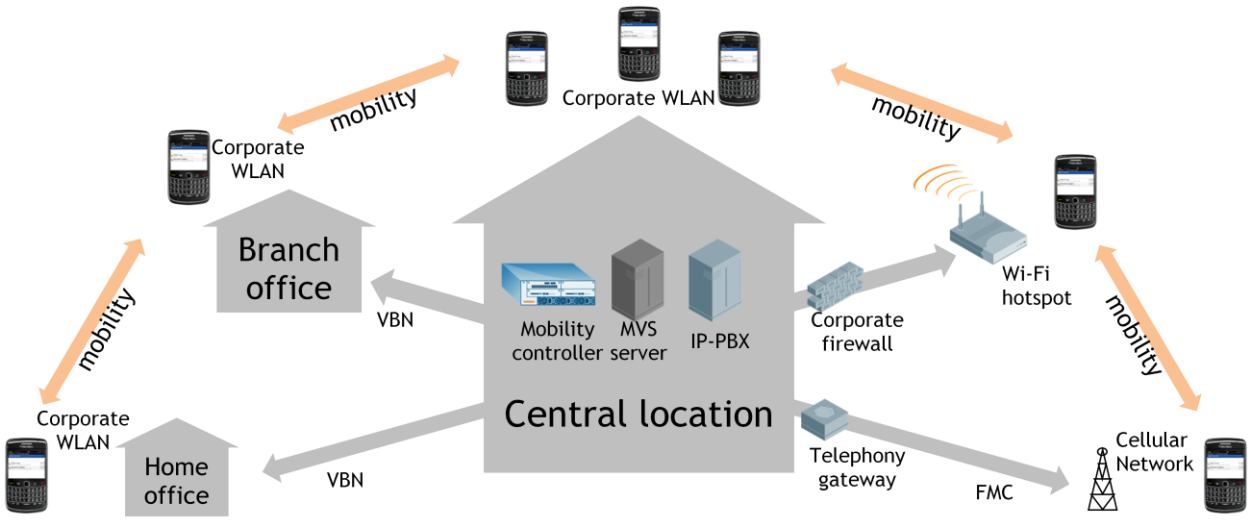



Figure 5. MVS architecture showing access options

The diagram above shows various means by which the BlackBerry smartphone can connect to its anchoring MVS Server in the corporate data center. Campus locations are served by a corporate WLAN with many thin APs, providing fully-authenticated and encrypted Wi-Fi connectivity. Smaller locations are served by Aruba's VBN technology. Providing the same level of secure corporate access, VBN connects APs in home offices and hybrid wired-wireless AP clusters in branch offices to the central site via secure encrypted tunnels. In public Wi-Fi hotspots, a VPN connection is required to support the BlackBerry MVS solution.

### 1.10 Other features and functions

In addition to “move call”, BlackBerry MVS supports a number of telephony features, such as voicemail integration. This involves automatically routing unanswered incoming calls to corporate voicemail, setting and clearing the message waiting indicator (MWI) on the BlackBerry smartphone, and enabling single-button voicemail retrieval. Features such as email notification, and distribution of voice messages are transparent to MVS, and will work as before.

Call transfer, call hold and other mid-call features are mediated by the BlackBerry MVS Server but executed by the IP-PBX. Their functionality will depend on the IP-PBX implementation and BlackBerry MVS Server integration. The BlackBerry contact list can be integrated with the corporate directory using BlackBerry Enterprise Server functionality.

Offloading data services to Wi-Fi is already a feature of the BlackBerry smartphone, and can be used independently of the BlackBerry MVS solution. The smartphone can be configured to automatically connect to the corporate WLAN when available, and use this connection for email, Web and other data traffic.

### 1.11 Security

The BlackBerry smartphone is synonymous with corporate security, and BlackBerry MVS uses proven security techniques.

- Corporate WLANs use WPA2-enterprise for authentication and encryption. This is RADIUS-based 802.1X authentication and AES encryption with unique user keys for all over-the-air traffic.
- When accessing features over a public Wi-Fi hotspot, VPN is necessary for security and privacy. The use of VPN clients is important for security, but they require administration, and can impact performance. A secure connection to the corporate WLAN is preferred over Wi-Fi hotspot / VPN access.
- All voice signaling traffic between the BlackBerry smartphone and BlackBerry MVS Server uses a proprietary protocol protected by end-to-end 3DES or AES-256 bit encryption.
- The BlackBerry smartphone already incorporates password-activated device access, on-board data encryption and ‘remote wipe’ features to protect corporate data that may be stored on the device.

In addition, the BlackBerry MVS solution will be attractive to many security-conscious organizations because it is capable of requiring that all calls pass through the IP-PBX. This allows a full call data record (CDR) list of all calls placed and received in cellular and WLAN coverage. It also allows the recording of cellular calls using the same system as extension-based calls. All the IP-PBX’s least-cost routing and call barring features also operate on these calls.

### 1.12 Device management

The BlackBerry Enterprise Server already allows BlackBerry smartphone configuration files to be packaged by the IT group and pushed to client devices. This is an important capability for reducing helpdesk calls and ensuring full security and usage compliance throughout the enterprise. Configuration for BlackBerry MVS functions is added to the existing device management suite.

### 1.13 The BlackBerry MVS value proposition for the enterprise

The BlackBerry MVS solution offers enterprises productivity benefits, opportunities for cost control and a remedy for areas where cellular coverage may be inadequate.

### 1.14 Productivity

BlackBerry MVS enhances the productivity benefits of the BlackBerry smartphone. As a purpose-built corporate productivity tool, it already offers email, corporate directory service, and integration with many enterprise applications such as those from Microsoft, IBM, Oracle and SAP software. BlackBerry MVS also allows the corporate IP-PBX to become the hub for all voice communications, bringing campus communications capabilities to remote employees. For the employer, whether originating or answering calls, voice services are seamless and comprehensive.

- Single-number identity. Business contacts can dial the employee using a single number and complete the connection whether over cellular or Wi-Fi. Outgoing calls will reflect the same "calling number" and so can be automatically saved to contact lists, while "call-back" features operate correctly.

- Single voicemail. Because all incoming calls transit the corporate PBX, they will be directed to corporate voicemail if unanswered. None will end up in the cellular operator's voicemail system, so the employee receives all messages in one voicemail box and can retrieve them with single-touch access. Prompt message waiting indication is provided whether in cellular or Wi-Fi coverage.

- The BlackBerry MVS Client integrates corporate extensions in the contact list, and provides presence information for corporate users (depending on the corporate IP-PBX or IM system). Other corporate users can be reached with simultaneous ringing of their smartphone and desk phone if desired.

- Calls can be moved between the WLAN and cellular networks, to a desk phone or any other number, offering call continuity when coverage on one network becomes unsatisfactory.

- Seamless connectivity allows IT groups to design communications-enabled business processes (CEBP) to encompass all types of network connection and deliver to remote employees useful communication tools that improve customer satisfaction. This can be particularly advantageous for branch office and mobile workers who receive a majority of calls from customers.

### 1.15 Cost control & savings

For the IT group, BlackBerry MVS improves control over cellular devices and costs in a number of ways:

- Outgoing calls are routed by the IP-PBX using the appropriate least-cost routing, and at landline carrier rates that are still considerably lower than on cellular networks, especially for international calls.

- When the caller is away from the office, particularly on international trips, Wi-Fi access avoids international roaming charges.

- Since calls made over Wi-Fi are diverted from the cellular network, cellular contracts can often be reduced (e.g. from 1,000 to 500 minutes/month), for corporate cost savings.

- All calls can be routed via the corporate IP-PBX, enabling full call logging and CDRs, and recording if required.

- Configuration templates pushed from the BES reduce user configuration errors and reduce calls to the helpdesk.

- Many cellular carriers offer “friends-and-family” or “favorites” plans where calls between designated numbers attract lower tariffs, or don’t count against monthly minutes. Adding the BlackBerry MVS single-number to such a list may reduce billed cellular minutes, thus reducing costs.

### 1.16 Coverage

Most employees still experience coverage gaps in cellular networks, and when these affect their workplace or home, they are the source of considerable frustration. The BlackBerry MVS solution allows IT to compensate for poor cellular coverage in campus and branch offices by using the corporate WLAN, while employees can self-install an enterprise Wi-Fi AP at home. Wherever the smartphone sees the corporate WLAN’s service set identifier (SSID), it will automatically connect, with no user re-configuration.

### 1.17 Designing the WLAN for MVS

State-of-the-art WLANs allow users and devices to connect to the enterprise network without cables, securely gaining access to corporate services on the core network. Wi-Fi is a new layer in the network that logically acts as a mobility overlay on top of fixed network equipment and fulfils the requirements of security, mobility and convergence without requiring major upgrades to the existing network infrastructure of routers and switches.

### 1.18 WLAN architecture for enterprises

Modern WLANs use the “thin AP” model. Thin APs include radio hardware and processors, but receive their software image, configuration and management functions from centralized mobility controllers. In use for several years, this architecture allows effective, centralized AP management, scalability, configuration control and upgrades. This is especially advantageous to meet the needs of high reliability and security within distributed enterprises with extended WLANs. Thin APs can be deployed as an overlay on existing LAN switches because on power-up they automatically discover their parent mobility controllers and set up on-demand encrypted tunnels across any LAN or WAN. No reconfiguration of VLANs or other changes to the existing LAN are required when adding the WLAN overlay.

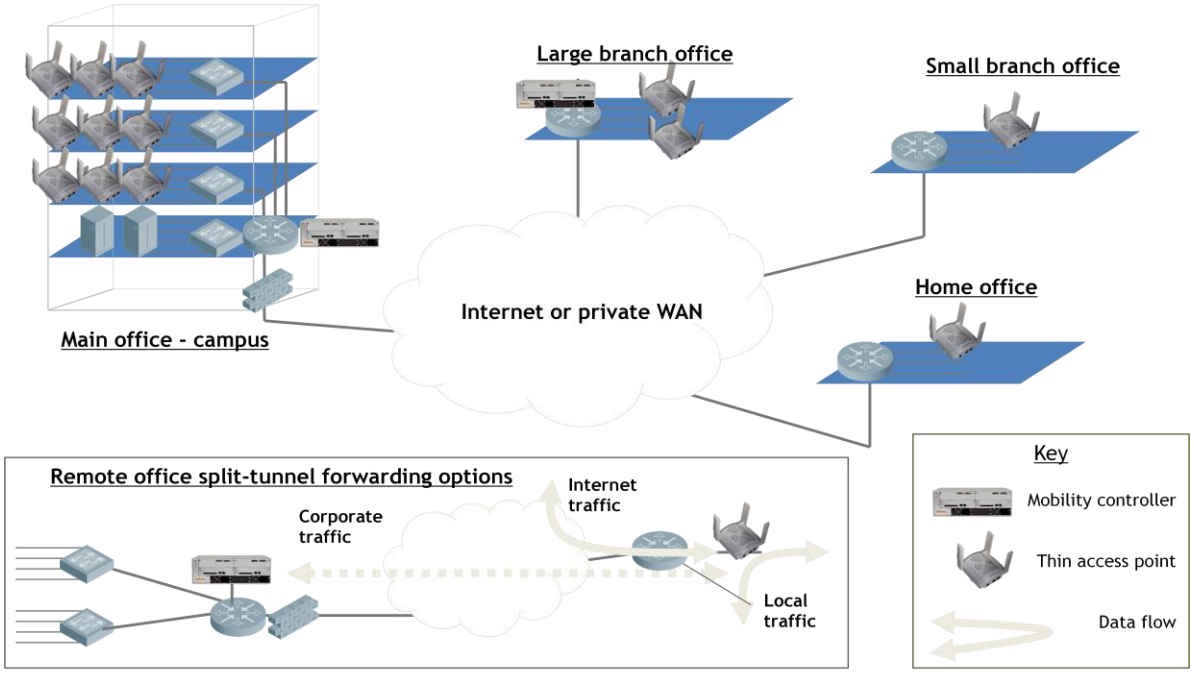



Figure 6. Aruba WLAN campus and wide-area topology options

WLAN mobility controllers aggregate traffic from APs, inspect and police that traffic, and deliver it to the core LAN. Because they handle traffic from hundreds of APs and thousands of users, mobility controllers are typically positioned in data centers, to create a controlled environment and provide access to the high-speed core network. Mobility controllers are high-performance networking platforms built specifically to run centralized WLAN functions such as thin AP management, automatic RF management, client management, 802.1X authentication, encryption, intrusion protection and seamless roaming between APs and mobility controller domains.

WLAN access points serve as distributed traffic collectors, tunneling wireless traffic to mobility controllers over wired networks. Access points provide radio coverage and user connectivity services while simultaneously serving as surveillance devices that constantly monitor the air for radio-based security threats. They also implement distributed functions such as adapting to local RF conditions, encrypting local traffic forwarding, and performing rogue AP detection and containment.

Software running on the mobility controller gives administrators a single point of control from which to locate and shut down rogue APs, load-balance traffic, detect coverage holes and interference and create role-based security policies that follow individuals as they move across the network.

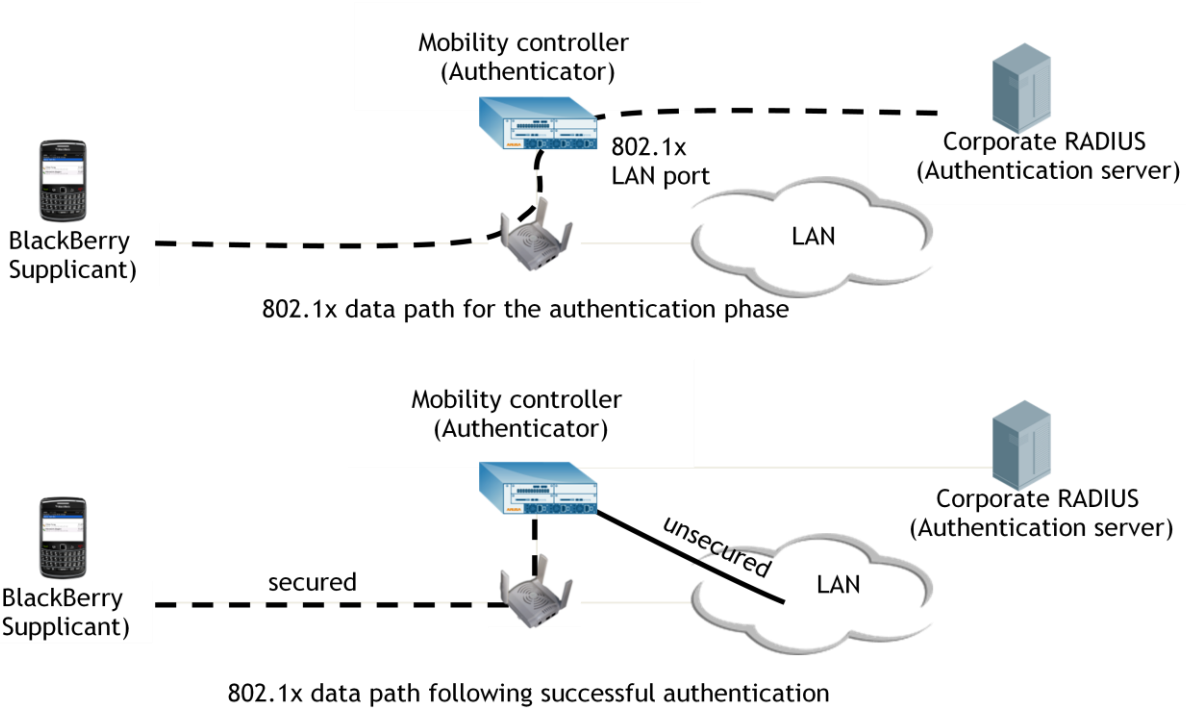



Figure 7. Authentication using WPA2-enterprise (802.1X)

For security, the WLAN uses the concept of identity-based authentication. Mobile users and devices by definition do not connect to the network through a fixed port. For this reason, the network must identify every user and device that wishes to gain access. Once this identity is verified, custom security policies may be applied to the WLAN so that access is provided appropriate to the needs of the user or device. The architecture used is 802.1X, based on RADIUS servers and a corporate directory service. The 802.1X standard has been a feature of WLAN architectures for some years, and is now being adopted by wired networks.

The standard for Wi-Fi encryption is the Advanced Encryption Standard (AES). The AES cipher is a very secure encryption algorithm mandated for U.S. government and military networks: it uses a 128-bit key to operate on a 128-

bit block of data, performing multiple passes or 'rounds' before encryption is complete. Each key is unique to the client and access point, lasts only for the duration of the association, and is rotated at intervals.

Aruba's implementation of a centralized WLAN architecture offers two encryption options. "Centralized encryption" is provided end to end between a remote client and the mobility controller in the corporate data center. For example, if a BlackBerry smartphone is connected to an Aruba Remote Access Point (RAP) in a home office, all its data and voice traffic is AES-encrypted over-the-air and across the Internet all the way to the mobility controller in the data center. In topologies where traffic is not centralized, "distributed encryption" is maintained over-the-air between the client and its associated AP, then the traffic is routed directly from the AP's LAN to its destination. Both centralized and distributed encryption use WPA2-enterprise with AES.

### 1.19 WLAN requirements for the BlackBerry smartphone and voice traffic

The BlackBerry smartphone differs from PCs on the WLAN in two respects. It is a handheld, battery-powered device, and it generates real-time-sensitive voice traffic. This section reviews the requirements for optimal support of BlackBerry smartphones on a WLAN, and explains Aruba's voice-specific features for the BlackBerry MVS solution.

The general requirements for handheld devices are to deliver the maximum battery life, and to correctly manage both voice and data traffic to and from the same device. Meanwhile, voice requires attention to quality of service (QoS) features and inter-AP handover. Finally, because it offers inside-the-firewall access to wireless devices, security is a paramount consideration for the WLAN, so security aspects of BlackBerry MVS are revisited.

#### 1.19.1 Features for best battery life

Smartphones need to balance performance against size, weight and battery life. RIM has always focused strongly on battery life and used many techniques to minimize data traffic and processor cycles. As a result, the BlackBerry smartphone is very frugal in power consumption. Nevertheless, adding a Wi-Fi interface will inevitably increase power consumption, and it is important to minimize the extra drain on the battery.

There are two main causes of power consumption in Wi-Fi. One is when the radio is switched on and in receive mode. Because the Wi-Fi protocol is largely unscheduled, it is difficult for the phone to know when it needs to be listening on the air, and anything that can be done to minimize this uncertainty will extend battery life. As we shall see, sleep modes involve the smartphone instructing the WLAN to buffer downlink frames for a while, then waking periodically to listen to beacons containing traffic notification flags.

The second source of power drain is when frames are transmitted. Fortunately, in this case the infrastructure is always-on and capable of receiving, so the smartphone does not need to coordinate with the WLAN when it has data to send. While the power used during very short transmission bursts is much higher than when in receive mode, the latter operates over much longer time periods, and deserves equal attention.

Features implemented by Aruba to reduce battery consumption include:

- On-call optimized sleep mode with the Wi-Fi multimedia-power save protocol (WMM-PS). This standards-compliant technique stretches to a maximum the period between frames when the client can sleep. Since voice frames are frequent and periodic (usually every 20 milliseconds), WMM-PS is client-triggered. When a new frame is generated internally, the smartphone sends it, and receives a buffered downlink frame from the AP immediately afterwards. Following this, it can return to sleep mode for the remainder of the 20 millisecond interval before the next frame is transmitted.

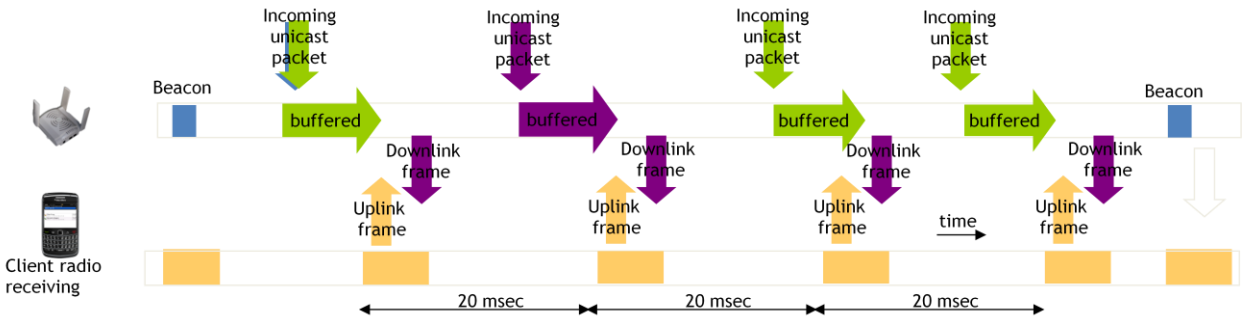



Figure 8. WMM-PS operation (802.11 U-APSD)

- Traffic filtering. Since an AP acts as a LAN bridge, all broadcast traffic on its subnet is re-transmitted to every wireless client. Because much of this traffic is not required by devices such as the BlackBerry smartphone, Aruba developed a feature that can filter out traffic by protocol. Reducing unnecessary traffic to the phone minimizes the time a smartphone's Wi-Fi radio is switched on and the number of acknowledgements transmitted.

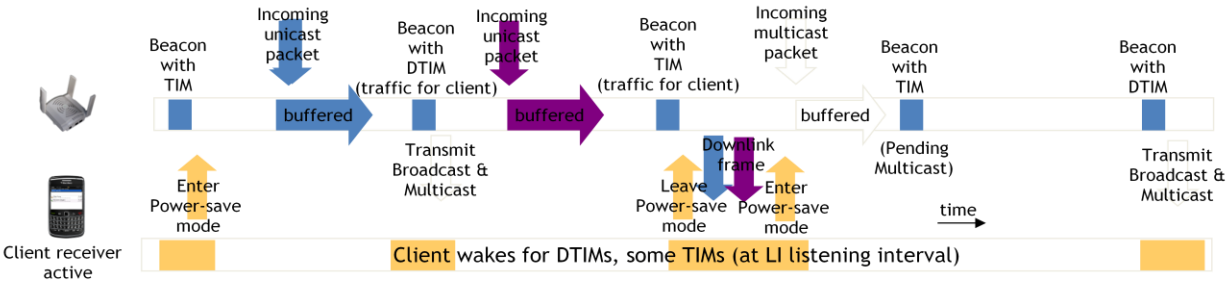



Figure 9. 802.11 Power-save operation

- Proxy ARP. The volume of ARP traffic increases as the number of devices on a subnet grows. Rather than forwarding every such request to the smartphone, the WLAN responds on its behalf, and minimizes the traffic sent to the smartphone to extending battery life.

- Modulation rate optimization, and retry minimization. Wi-Fi is an adaptive protocol, with algorithms that change the modulation rate to send data as fast as possible, consistent with low error and retry rates. When these algorithms are well-tuned, there is a higher probability of first-time success, and a lower retry rate minimizes phone activity. The same thing applies when transmitting at a higher rate. For example, transmitting at 24 Mbps rather than 6 Mbps reduces the time taken to send a frame and minimizes power consumption. Aruba employs a number of techniques that minimize error rates for voice transmissions and optimize retry behavior.

- Tuning for maximum on-hook sleep periods. The Wi-Fi standards include a number of options for extending sleep mode for voice clients. Aruba favors extending the delivery traffic indication map (DTIM) timer, which increases the client's sleep time. During these sleeping intervals, the WLAN buffers downlink traffic. If there is anything to send, a notification flag is set in the DTIM, which the client must wake to monitor. This is an effective battery-extension mechanism, but increases the delay in ringing and answering an incoming call, if it is extended too far. Generally, with a 100 msec beacon interval, a DTIM every two beacons represents a good compromise.

### 1.19.2 Features for best quality of service

Most users have an intuitive grasp of overall QoS – they can tell a good call from a bad call by listening to it. But from inside the network, things are a little more complicated. Several factors such as end-to-end delay, jitter, lost and errored frames can all contribute to quality impairment. The endpoint codec in use is also significant. A poor codec determines the upper limit for intrinsic quality, even under good conditions. Conversely, a good codec is able to elide, or smooth over errors to compensate for transmission loss and jitter in the network.

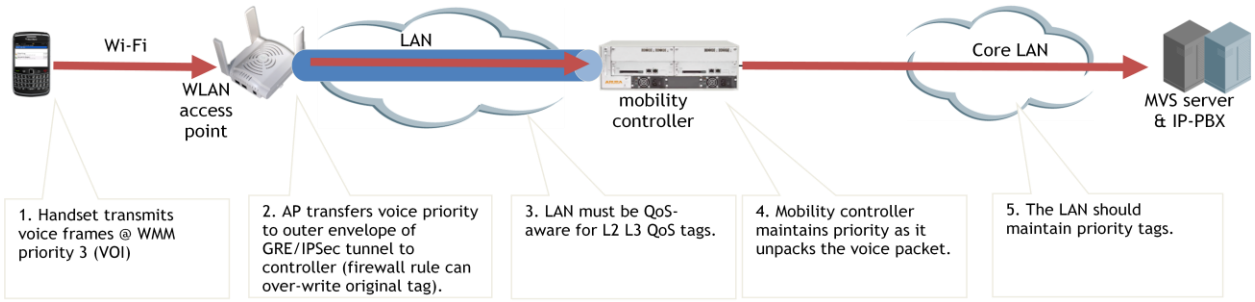



Figure 10. Upstream QoS chain for Aruba WLAN carrying MVS traffic

VoIP calls in an enterprise network often traverse a long chain of switches, routers and WAN connections. The Wi-Fi link is only one segment of the end-to-end call, but a critical one, because wireless is an inherently variable medium and is subject to interference and RF fluctuations.

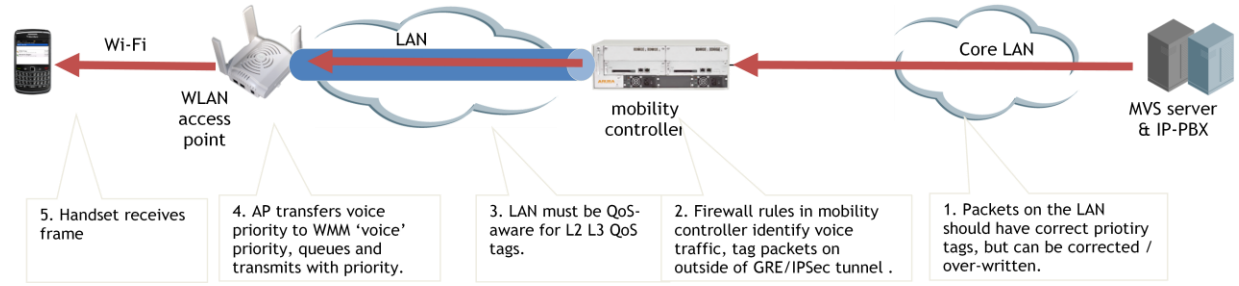



Figure 11. Downstream QoS chain for Aruba WLAN carrying MVS traffic

Aruba's uses a two-fold approach for VoIP. First, every step is taken to ensure that voice frames get priority over the air, and are received accurately with as few retries as possible. Second, monitoring tools allow network managers to visualize the voice activity in the network. Quality metrics and diagnostics help to ensure that their voice services are running smoothly, and accurately localize impairments if quality levels should sag.

- The first stage of designing a WLAN for the best QoS is to utilize the 5 GHz band as much as possible. This band has more RF channels and less interference from other equipment such as microwave ovens and cordless phones than the 2.4 GHz band. The BlackBerry Bold 9000 is dual-band capable, and Aruba has a band-steering feature that will automatically move such devices to the higher band where available, giving them the opportunity to work in a "cleaner" medium for better performance.

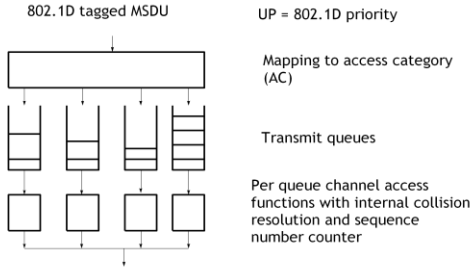
- Other devices like the BlackBerry Bold 8700 only operate at 2.4 GHz. When these devices are used, the objective should be to move other devices such as PCs to the 5 GHz band, leaving the 2.4 GHz band as empty as possible for the best performance. This is part of Aruba's standard Adaptive Radio Management (ARM) capability, which maximizes the WLAN's data capacity by utilizing all RF channels.

- While the measures above are important, enterprise access points always carry a mix of high-priority voice and lower-priority data traffic. The Wi-Fi protocol prioritizes frames using the WMM protocol. WMM

ensures voice traffic gets preferential access to the air, so when both voice and data frames are queued for transmission, the voice frame will get on the air first. WMM has been used for several years, and has proved to be very effective in practical networks. It ensures that even when an access point sees an overwhelming volume of data frames, the voice traffic will get through successfully.

| Priority | 802.1D Priority (= UP) | 802.1D Designation | Access Category | WMM Designation |
|---|---|---|---|---|
| increasing | 1 | BK | AC_BK | Background |
| | 2 | - | | |
| | 0 | BE | AC_BE | Best Effort |
| | 3 | EE | | |
| | 4 | CL | AC_VI | Video |
| | 5 | VI | | |
| | 6 | VO | AC_VO | Voice |
| | 7 | NC | | |

Mapping WMM access classes to 802.1D DiffServ priority




Linkage from 802.1D to WMM in a station

Figure 12. Prioritization and end-to-end tag continuity using WMM

- The WMM protocol includes a table that maps the priority tags used in the wired LAN to the Wi-Fi layer, and in most networks this mapping is sufficient. The WLAN identifies high priority traffic because it already carries a high-priority tag. But many networks harbor discontinuities in which packets lose their tags, such as when they have travelled over the Internet or transited a device that lost the tag information. This effect is prevalent enough for Aruba to build a feature where the mobility controller's or AP's integral firewall monitors traffic and re-sets or over-writes priority tags based on protocol, source or destination. This ensures correct prioritization across the WLAN and for onward transmission.

- When voice traffic approaches the limits of an access point's capacity, it is necessary to implement call admissions control (CAC) to prevent further voice calls from causing overload. While CAC is not as important now that phones use 802.11g and 802.11a, it is an important network design consideration. Aruba has two approaches to CAC. First, a number of indicators from the integral stateful firewall are used to count the number of active voice calls on an access point, and detect when overload is approaching. Following this, it is possible to block further calls by a variety of means.

- However, it is preferable to engineer the network so CAC limits are very seldom approached, and the mechanism to achieve this is inter-AP load balancing. In addition to balancing across frequency bands, ARM balances all devices across the available RF channels within a band to ensure that no AP is overloaded compared to its neighbors. This helps to reduce retransmissions and avoids hitting call admissions capacity limits. Aruba access points can also be configured to advertise current load and available admissions capacity, allowing the smartphone to select a suitable access point for handover.

- Aruba includes a number of powerful diagnostic tools for voice services. In the BlackBerry MVS architecture, signaling streams are encrypted and are opaque to the WLAN, but media streams use the RTP and RTCP protocols. These are monitored for quality by both explicit (when RTCP is present) and implicit means, giving the network manager per-call figures for voice quality.

- Another consideration for user-perceived QoS is general WLAN coverage. Many WLANs are designed with PC use in mind, offering coverage in places where nomadic employees may sit and work. But BlackBerry smartphone users are truly mobile, so it is important to identify areas where walking, talking users will need service, and to ensure they are covered. This may include pathways between buildings, elevator shafts, stairwells and corridors. Aruba provides a number of tools for RF planning, and also dynamically calculates heat maps to visualize coverage.

- Aruba's ARM capability continually optimizes coverage based on measurements of signal strength and interference reported by WLAN access points. ARM acts to maximize coverage and network capacity, while avoiding interference: all these features contribute to optimizing voice quality.

### 1.20 Managing voice and data traffic from the same device

As a business-oriented device, the BlackBerry smartphone transmits and consumes a large quantity of data as well as voice traffic. As noted above, it is important for the WLAN to separate the frames, giving voice priority over data, and also providing filtering and firewall features to ensure appropriate access to corporate resources.

Many WLAN architectures find this difficult to accomplish, as they statically map each WLAN SSID to a single VLAN, and subsequently identify traffic as voice because it is on the voice SSID and VLAN. If a smartphone were to be mapped to the voice VLAN, how would its data needs be accommodated? Or if it were on the data VLAN, how would its voice traffic find a destination?

In Aruba's mobility architecture, the device is identified as a voice/data device, and placed in a role that defines its data and voice characteristics separately. Individual session streams are identified and subject to appropriate stateful firewall rules, based on protocol, source and destination addresses. For example, voice frames are tagged for high priority and preferentially queued when destined for another defined voice address, while data is assigned a lower priority. Identity-based authentication and role management, and session-based policing are key attributes for a mobility network such as the BlackBerry MVS architecture.

Thus, in Aruba's architecture, the BlackBerry smartphone can connect on a multi-purpose SSID, or one with parameters optimized for battery-powered handheld devices. Each traffic stream generated and received by the smartphone will be classified, prioritized and policed separately, regardless of the SSID or VLAN context.

For transmitting frames over-the-air, the BlackBerry smartphone's QoS implementation is superior to most smartphones available today. It classifies voice and data traffic with appropriate WMM priorities, assuring uplink frames have the correct QoS. The Aruba WLAN is responsible for maintaining and policing tags in the upstream direction, and also for all traffic prioritization on the downlink to the smartphone. This combination provides the best implementation for end-to-end QoS.

### 1.21 Inter-access point handover

Handover for voice calls is a very simple concept. A phone is on a call while associated with a particular AP. Either because of movement or RF signal degradation, the current AP becomes a poor choice, so the phone moves its association to a new AP from which it receives a better signal. Handovers are frequent – a fast-moving smartphone might execute an AP handover every 30 seconds on a walk through a typical enterprise WLAN. The key metric for successful handover is also clear. There is a gap in the audio signal from the time when the phone severs its association with the first AP, or the connection becomes unusable, until it re-establishes the media stream on the new AP. The target metric for this gap is 50 milliseconds if it is not to be perceptible to the listener, while a figure of more than 500 msec will usually cause complaints. Wi-Fi technology has already surpassed the 50 msec goal, which is routinely attained under controlled conditions, but work continues to improve techniques and decrease the average and worst-case handover latency.

With the advent of centralized WLAN architectures, some of the techniques from cellular technology are being adapted for Wi-Fi. However, in the prevailing model the client makes handover decisions, aided by information from the network. Also, while standards cover the format and use of frames exchanged over the air, many of the

algorithms critical to handover performance are not specified and are up to individual designers of phones and the WLAN infrastructure. While good WLANs can improve the handover latency for any phone, they cannot turn a poor client implementation into a good one.

Fortunately the RIM has a very good set of handover algorithms that have been proven over several years by dual-mode phones such as the BlackBerry 8820, introduced in 2007 and tested and supported on the Aruba infrastructure since that date. A typical handover event passes through the following sequence:

- Develop a list of handover candidates. The smartphone passively monitors AP beacons, and periodically probes on different RF channels to discover neighboring access points. As signal strength on the current AP falls, active probe requests are increased to ensure accurate and current information. (The new 802.11k neighbor report allows the AP to explicitly advertise handover candidates; this is supported by Aruba but not yet certified for interoperability by the Wi-Fi Alliance.). BlackBerry smartphones generally make good handover target selection, choosing the candidate with the strongest signal at the instant of handover.

- Decide when to handover. While many smartphones are "sticky", staying with the current access point too long as its signal deteriorates, the BlackBerry smartphone makes very timely decisions to initiate handover, generally at a signal to noise ratio (SNR) of around 25 dB.

- Execute the handover. A "full" handover, the default mode, is just like an initial authentication event. The client starts from scratch, establishing its identity and deriving new keys. With WPA2-enterprise protocols such as PEAP/MSCHAPv2, this requires around 50 frames over-the-air. In this phase, the responsiveness of the AP is most important. Even small delays can build up to a large handover gap, as voice frames cannot resume until after the authentication. Fortunately, a BlackBerry smartphone performing full authentication on Aruba infrastructure is faster than any other smartphone at around 240 milliseconds.

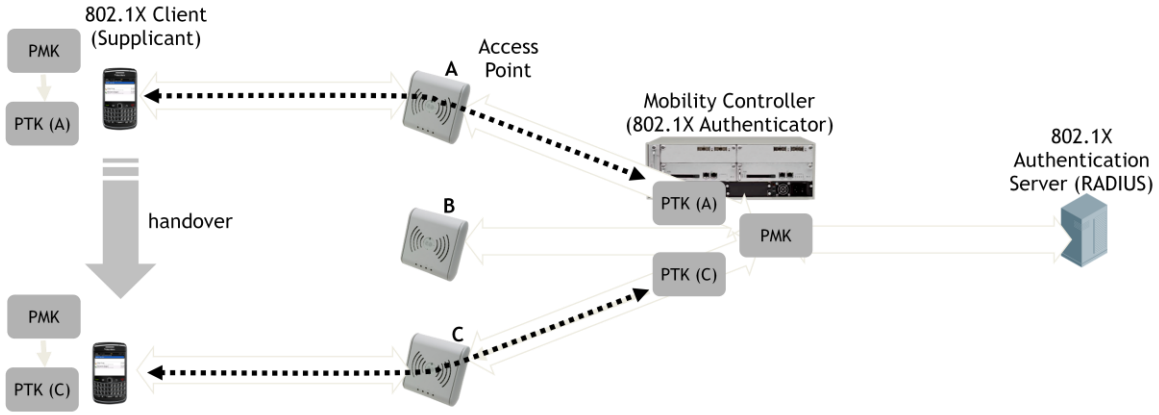



Figure 13. 802.11i PMK caching handovers in Aruba's architecture

- There are several possible shortcuts to the full authentication sequence. When the phone has previously authenticated to an AP, it can use 'PMK caching' to re-establish association based on cached master keys. PMK caching is supported by both Aruba and RIM, and results in handover times of sub-50 milliseconds.

- A newly ratified standard, 802.11r will allow a technique similar to PMK caching to be used for any AP in the same WLAN, so only the initial association would require a full authentication. Both Aruba and RIM are working towards an interoperable 802.11r implementation under the auspices of the Wi-Fi Alliance.

- An alternative solution to reduce handover latency is to apply a lesser standard of security. WPA2-personal uses the same level of encryption as WPA2-enterprise, but shared rather than individual keys. This enables

handover performance similar to PMK caching with WPA2-enterprise, but will not be acceptable to all network security officers.

- Aruba has extensive experience tuning handover mechanisms in conjunction with BlackBerry smartphones, and the combination delivers one of the fastest, smoothest handovers in the industry. The new features emerging from the IEEE standards group in 802.11k, r and v will enable handovers to be swifter and even more precise.

### 1.22 Security

Today's wired enterprise networks are primarily built with a fixed edge where users and devices connect to the network by plugging a cable into a port in the wall. Security in such a fixed edge network is applied to ports in order to protect the network from unauthorized users and devices. Encryption is seldom used, as it is assumed that intruders cannot gain physical access to Ethernet outlets, and so cannot monitor or interdict traffic – an assumption that is not valid today, if indeed it ever was.

WLANs stand apart from wired networks as they enable mobility, a concept that drives the need for identity-based networking instead of a port-based scheme. Since wireless users can roam across multiple ports on a network, port-based security models do not apply to the WLAN-connected client. Mobility breaks the fixed edge concept of port-based networking. Identity-based security, though more complex, is far more granular than port-based security, since it applies policies at both the user and device levels.

Some WLAN vendors link security to the SSID, mapping each SSID to a VLAN and relying on VLAN separation for security. This is a cumbersome and limiting approach, as large-scale VLAN deployments are complex and simple configuration errors can open vulnerabilities. Aruba incorporates an integrated stateful firewall in its mobility controller that can identify each user and device as it roams. The result is true identity-based security with pervasive mobility.

Since it is assumed that an intruder is constantly monitoring over-the-air traffic in a WLAN, Wi-Fi has evolved with excellent security. Wi-Fi's WPA2 security framework has yet to be broken and offers considerably greater security than nearly all wired LANs. Modern enterprise WLANs all implement WPA2 security, as do current Wi-Fi client devices such as the BlackBerry smartphone. However, Aruba adds two architectural enhancements that are of value in the enterprise environment – centralized encryption and an integrated policy-enforcement firewall.

- Centralized encryption is an option used by Aruba in campus and remote deployments where a Layer-2 GRE tunnel is set up between the dependent access point and its parent mobility controller. In this scenario, the mobility controller and client – rather than the access point and client – are the encryption endpoints. Traffic on the northbound mobility controller interface is unencrypted, but since the mobility controller usually resides in the data center, this is usually acceptable. All WLAN data traversing the distribution portion of the LAN will be encrypted.

- Aruba's integrated firewall is an International Computer Security Association (ICSA)-certified stateful firewall capable of identifying sessions by source, destination address, and protocol. The firewall allows the network administrator to place custom limits on individual user access. Different categories for employees, contractors and guests can make use of the same network, even though each group only has access to the information they are authorized to view. For instance, a certain class of user might be given access to a particular server using one or two protocols, but only for certain hours of the day. Others might be allowed to transmit only voice traffic, or other protocols. Linkages between the WLAN and the firewall functions

allow custom security policies to be applied to the network so that only access appropriate to the business needs of the user or device is provided.

- The firewall can be considered a second line of defense behind Wi-Fi authentication. Knowing the limits on a user's activity – either from RADIUS attributes learned as part of WPA2-enterprise or from internal configuration – the mobility controller monitors all protocol streams passing over the WLAN to ensure that they meet the user's profile. If violations are detected, events are logged and alarms are raised. In the event of repeated violations, a user can be automatically de-authenticated and blacklisted.

Aruba's industry-leading security architecture lets IT managers define policies on a per-application, per-user basis for wired and wireless networks of virtually any size. Features include flexible authentication, high security encryption, and integrated network access control (NAC) for restricting unauthorized access. Aruba is the only wireless LAN vendor with products that are compliant with ICSA Labs, Common Criteria, FIPS 140-2, and DoD 8100.2. Aruba is the first vendor to receive accreditation from the U.S. Army's Office of Information Assurance and Certification for an 802.11n wireless LAN solution.

### 1.23 Conclusion

RIM's introduction of the BlackBerry Mobile Voice System represents a landmark in the development of enterprise-centric FMC/UC architectures. Because RIM designs the BlackBerry Enterprise Server, a server already in the corporate data center, in addition to the popular BlackBerry smartphone, the company is in a position to closely coordinate software on the client with a call anchor point within the enterprise.

But as many FMC designers have discovered, the Wi-Fi layer is not transparent and not all WLANs are equal. End-user acceptance depends on the overall quality of experience, freedom from interference and interruptions, expeditious handovers and roaming, good battery life and predictable coverage.

For business-critical BlackBerry MVS deployments, an Aruba WLAN offers the highest levels of security and performance. Employees at home and in branch offices benefit from remote APs, part of the Aruba VBN architecture, allowing them to extend Wi-Fi coverage without any complex configuration of the BlackBerry smartphone.

Meanwhile the network manager has access to the many visualization and diagnostic tools required to assure service quality without increasing helpdesk support.

The combination of BlackBerry MVS with an Aruba WLAN enables mobile employees to access the same rich information and ease of communication that they currently experience at their corporate desks. As an ever-higher proportion of the workforce moves away from corporate offices, BlackBerry MVS is the tool that will allow them to stay in touch with their teams.

### 1.24 References


1. 'Defining the virtual workforce', Melanie Turek, Nemertes Research, January 2005 http://www.nemertes.com/managing/defining_the_virtual_workforce

2. 'Enterprises could be wasting £264m per annum on mobile call costs', Damovo UK Ltd, November 2009 http://www.damovo.co.uk/documents/091116DamovoFMCresearchFINAL_000.pdf

3. 'Gartner's top 10 predictions for 2009', Gartner, February 2009, http://www.gartner.com/it/page.jsp?id=876512

**About Aruba Networks**

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.


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



WP_FMC_with_RIM_MVS _100423