

Enterprise



## **Fixed-Mobile Convergence with UMA for Enterprises**

Peter Thornycroft

---

# Approaches to Enterprise Fixed-Mobile Convergence

Advances in voice-over-IP (VoIP), and cellular networking technologies are driving opportunities for businesses to improve productivity while saving on telecommunication expenses. One fast-developing area, Fixed-Mobile Convergence (FMC) allows mobile phones to connect to Wi-Fi networks when available, taking advantage of the low cost, high bandwidth and extensive indoor coverage of Wi-Fi networks.

Within enterprise FMC there are several different architectural options that differ, depending on how closely the mobile phone is linked to the enterprise PBX, where the phone number is hosted and what voice and data calling features are offered on the phone. The different architectures can be classified into three categories:

## **PBX-centric**

In a PBX-centric architecture the corporate PBX is the anchor-point for calls. All incoming calls are directed to the PBX number (usually a direct inward-dial number as used by a PBX extension on a desk), and all outgoing calls are originated from the PBX, (the 'caller-ID' seen by the recipient is the PBX number). When a phone is within range of the corporate Wi-Fi, VoIP protocols connect it directly to the PBX, like a deskphone, and custom software on the phone allows it to emulate feature keys like the deskphone. When outside Wi-Fi coverage, the phone continues to act as a client of the PBX. An incoming call at the PBX is passed to the phone's cellular number for completion, whereas when an outgoing call is launched from the phone, it calls back to the PBX which then directs the call to the destination. While in communication with the PBX, the phone can provide many of the features of a deskphone.

PBX-centric solutions are designed and marketed by PBX vendors, and require the addition of custom software clients to the cellphone, and call-anchoring FMC software to the IP PBX server. Every PBX-centric solution is specific to a particular PBX product family: a phone set up to work with one vendor's FMC solution will not work with a solution from a different vendor. A PBX-centric architecture is likely to appeal to businesses where there is a strong, single-vendor IP PBX solution in place. They allow for the extension of useful PBX features as the user roams, whether in Wi-Fi or mobile coverage.

PBX-centric solutions are available from major suppliers including Alcatel, Avaya and Cisco.

## **PBX-independent**

Similar to PBX-centric architectures in that the equipment is owned by the enterprise and installed on-site, PBX-independent architectures are based on third-party adjunct servers that work with different types of IP PBXs. The server acts as an anchor point for call handover, but usually relies on the PBX and its telephony gateways to dial outside calls. This architecture uses special client software on the handset, primarily for Wi-Fi connection and handovers, but also provides PBX features and optionally presence and instant messaging (IM) capabilities.

Vendors with PBX-independent solutions include DiVitas, Agito and NewStep.

## **Carrier-centric**

While the solutions above are focused on equipment installed on an enterprise's premises and involve some level of integration with an existing IP PBX, mobile operators have followed a different path to FMC. They have focused on connecting mobile phones to Wi-Fi networks, but the phones continue to receive all their

services from the mobile operator. This approach allows consumers to compensate for poor in-home cellular coverage by installing a Wi-Fi access point, and depending on the tariff, to save money on calls made when in Wi-Fi coverage.

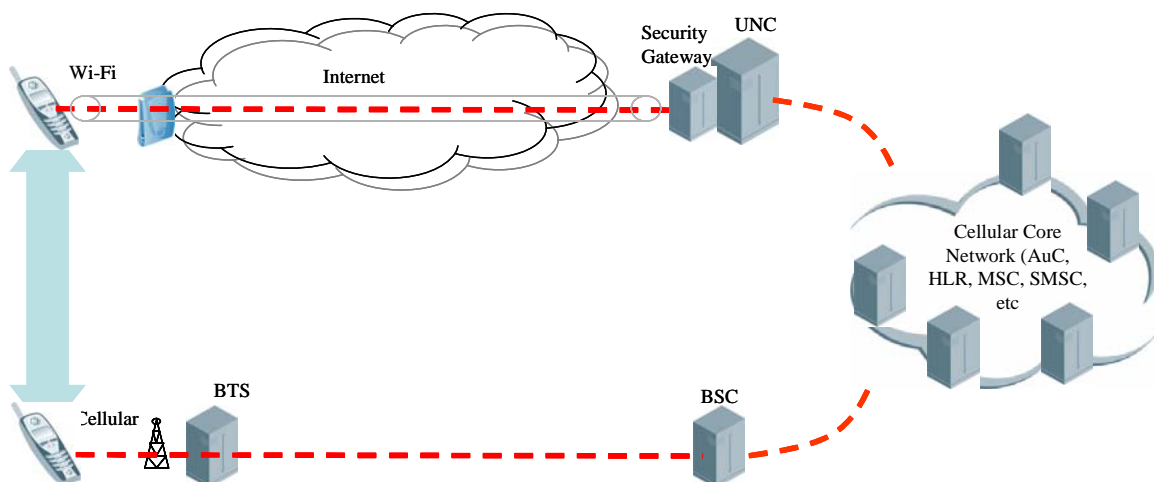
PBXs are not involved in a carrier centric architecture: the handset behaves as a standard mobile phone everywhere, and the subscriber continues to receive the same set of mobile services whether in cellular or Wi-Fi coverage. The mobile number used for all calls, but the cellular network transports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

The most successful form of carrier-centric FMC to date is known as UMA (unlicensed mobile access). UMA is a Global System for Mobile communications (GSM) standard and is in service with many GSM operators worldwide. Because UMA is a mobile industry standard, all major mobile handset vendors now offer UMA-enabled phones off-the-shelf. In the USA, T-Mobile offers a UMA service branded 'HotSpot @ Home'. While primarily marketed for use by consumers with residential Wi-Fi networks, HotSpot @ Home has several advantages for different business uses. Aruba Networks and Kineto Wireless have investigated how to best leverage UMA service, and this document is intended to assist enterprises as they evaluate FMC architectures and services.

## UMA architecture

UMA is a mobile industry standard that enables carriers to deliver mobile services over Wi-Fi networks. By deploying UMA, mobile operators can enable subscribers with UMA-enabled dual-mode cellular/Wi-Fi mobile handsets to automatically roam and handover between cellular and Wi-Fi networks. As subscribers transition between networks they receive a consistent set of mobile voice and data services.

From the mobile operator's perspective, UMA effectively turns Wi-Fi networks into seamless extensions of their outdoor cellular network. From the subscriber's perspective, UMA service enables them to receive high-performance, low-cost mobile voice and data services whenever their handset can connect over a Wi-Fi network.



---

The diagram above shows the basic architecture of a UMA service deployment. Installed in the mobile operator's core network, the UMA Network Controller (UNC) is a gateway between the mobile service core and the Internet. To the core mobile network, the UNC emulates a standard Base Station Controller (BSC), while on the Internet side it supports IP protocols, notably IPSec. When a UMA phone connects over Wi-Fi, it must first authenticate via the UNC to the mobile core network: this happens based on its Subscriber Identity Module (SIM), the small card identifying the user in GSM networks. Following authentication, a UMA phone establishes an IPSec tunnel to the UNC for GSM signaling, while voice conversations are carried using VoIP technology. The UNC translates these streams (signaling and bearer) back into the protocols recognized by the mobile core network.

Breaking this down in more detail, the exchange proceeds as follows:

- First the phone must recognize it is in range of a suitable Wi-Fi access point. This involves configuring an SSID and other parameters on the phone. T-Mobile UMA phones are pre-configured for the T-Mobile HotSpot @ Home Wi-Fi home router and public T-Mobile hotspots, but more can be added. The phone will automatically associate to these access points when they are detected;
- Following this the phone obtains an IP address through DHCP, and in establishing a connection over the Internet it negotiates the corporate firewall and traverses a network address translation (NAT) service;
- The phone must find the appropriate UNC security gateway (SeGW). This will be carrier-dependent: T-Mobile uses the Domain Name System (DNS). The phone requests a 'xxxx.t-mobilesgws.com' DNS lookup, and DNS then returns the IP address of the appropriate SeGW;
- The handsets use certificates to authenticate the SeGW. Currently operators use their own certificates so handsets are set up to always use the operator's own network. In time, operators may use certificates from popular certificate authorities, allowing handsets may roam between operators when using Wi-Fi;
- Next the phone connects to the UNC, specifically the SeGW, using Internet key exchange (IKE) to derive keys to set up an IPSec tunnel to the UNC. Thereafter, all communications over the Internet are encrypted;
- Within the IPSec tunnel, the UMA signaling protocol is very similar to that used over GSM. When a call is set up, it will use GSM codecs such as the adaptive multi-rate codec (AMR) over IP transport within the IPSec tunnel;
- Mobile data services such as short message service (SMS), multimedia message service (MMS) and the operator's mobile portals are also carried over UMA. SMS, MMS and other mobile operator services are always directed to the UNC and the mobile core, but depending on the handset and the carrier, it is possible for non-operator data services to reach the phone outside the UMA tunnel, e.g. Web browsing traffic from some phones can bypass the UNC;
- In UMA, handovers between the mobile and Wi-Fi networks occur in a similar fashion to handovers between cell towers on the outdoor mobile network. For example, when a mobile phone is on a call and connected over a Wi-Fi network in which the Wi-Fi signal degrades, the phone can signal to the mobile core network that it would like to handover to another cell tower. At this point the network instructs the phone to switch over to the target outdoor cell tower and the mobile network moves the voice call from the UNC to the BSC serving the target outdoor cell tower. In the early stages of development, most UMA phones assumed single, isolated Wi-Fi access points, and whenever the Wi-Fi signal deteriorated past a threshold, the phone would switch to cellular without looking for an adjacent access point. More recent phones are much better at inter-access point roaming, but may not incorporate all of the sophisticated handover features found in other Wi-Fi phones. Some UMA phones provide an option to enable or disable inter-access point roaming for each SSID in its list of Wi-Fi profiles.

---

## Using UMA with an enterprise Wi-Fi network

An enterprise with a state-of-the-art Wi-Fi network can support UMA phone service, providing benefits such as assured coverage, lower-cost calls and simple configuration. However, several hurdles must be overcome to match the capabilities of an enterprise wireless LANs (WLANs), which differ considerably from home Wi-Fi networks.

- **Security.** As an open medium, Wi-Fi is impossible to contain, and anyone deploying a WLAN must assume it can be monitored from outside the premises. Following an early false start with wired equivalent privacy (WEP), Wi-Fi networks secured with Wi-Fi protected access (WPA2) and 802.1x are considered more secure than most wired LANs. The challenge is to introduce UMA phones into a secure corporate environment without having the phone introduce a point of vulnerability;
- **Quality of Service.** Whereas WLANs that are not properly secured pose a threat, unreliable networks are useless. It is important that the UMA user's experience on Wi-Fi be satisfactory at a minimum, and that this new service does not adversely affect other WLAN users.

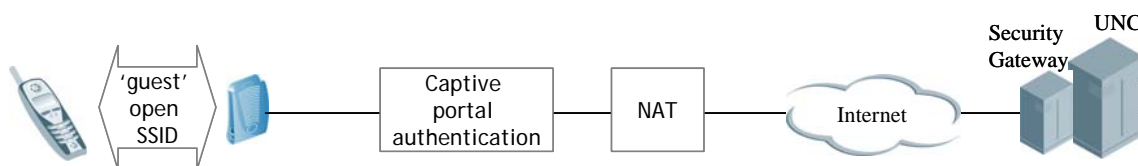
These potential issues can be mitigated in different ways, However, before addressing these issues we will turn first to a discussion about the level and type of access given to UMA devices, as these will inform the discussion about migration options.

### Firewall considerations

Most corporate WLANs offer secure network service to employees within the corporate firewall, providing access roughly equivalent to a wired Ethernet connection. Guest access for visitors to the enterprise is also provided, usually on an open SSID, and with a captive portal Web page for terms of service and/or login with guest credentials. Following guest authentication, traffic is typically directed outside the firewall.

UMA service can be enabled using either type of access, in the following ways:

### UMA over an 'open' SSID



- Either use an existing, open SSID, or configure a new one for the desired UMA carrier and service. Phones will need to be configured with the 'guest' SSID (but only once per phone) unless the SSID used is one of the carrier's 'well-known' SSIDs. For T-Mobile, two SSIDs are pre-configured on all phones: the HotSpot @ Home Wi-Fi router is 'XXXX' and the T-Mobile hotspot service is 'tmobile';
- The phone does not have the capability to negotiate captive portal Web pages, so it will be necessary for the Wi-Fi network either to identify that this is a UMA phone seeking service, or to remove the captive portal. Identification of UMA-specific traffic is explored later in this paper.

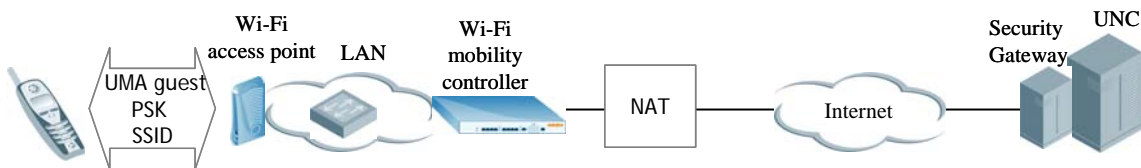
With this configuration, UMA service will be enabled over the corporate WLAN but isolated from the enterprise intranet. Note that using an open SSID implies either providing a completely open SSID with no captive portal, or a new SSID specifically for UMA service. Also, any UMA subscriber of the specific

---

carrier, e.g. T-Mobile, will be able to access service via the corporate WLAN even if they are not an employee of the enterprise or simply in range of the network. These considerations may make this a less attractive option to some network managers, but alternate deployment models are available to mitigate such concerns.

### UMA over a 'UMA guest' SSID

In this model, UMA traffic is still kept separate from the corporate intranet, but rather than allowing open, unauthenticated access to any device, the WLAN uses network-specific credentials that permit a network manager to restrict access to only enterprise-owned UMA phones. The simplest way to implement this is to use a pre-shared key (PSK) and either WPA or WPA2 authentication.



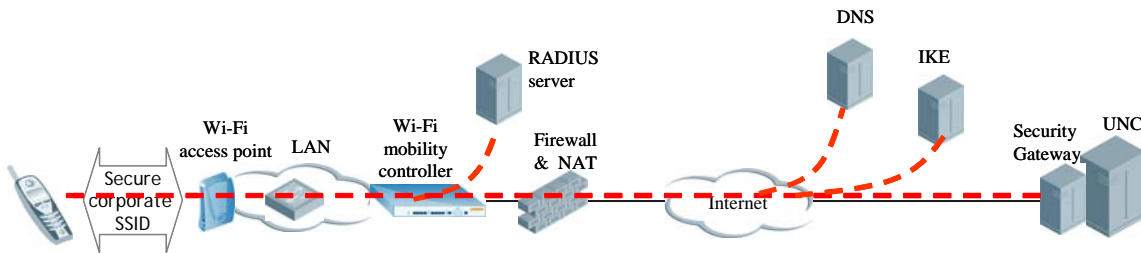
- Use an SSID for the desired UMA carrier and service with a WPA or WPA2 pre-shared key. Phones will need to be configured with these credentials, but only once per phone;
- Firewall or VLAN policies can be configured to allow devices on this SSID to communicate only with the UMA operator's SeGW. This means devices cannot use this SSID to gain intranet access except for UMA;
- Since UMA phones do not have the capability to negotiate captive portal Web pages, a firewall or traffic segregation policy takes the place of captive portal authentication;
- This approach is especially appropriate for UMA phones that are not 802.1x-capable.

The T-Mobile HotSpot @ Home service includes tools that allow easy phone configuration by corporate IT staff. Once an initial handset has been configured for the 'UMA guest' SSID, its settings can be forwarded to other HotSpot @ Home handsets simply by sending an SMS message to the new phones. The recipient can accept the configuration with a single key-stroke.

### UMA over an authenticated SSID

The alternate form of access is to use a 'normal' SSID on the corporate WLAN. The state-of-the art is to use WPA2 authentication/encryption with 802.1x, normally with keys derived from a RADIUS server. The goal of this deployment model is that phones should use the same level of security as laptop computers, a goal that is already attainable.

Some enterprises use a separate SSID for voice, while others prefer to have one SSID for voice and data services. The proliferation of smartphones generating both voice and data simultaneously makes this distinction moot. Indeed, the more important distinction today is the type of battery-powered clients used, since different settings may be useful for extending battery life on a 'handheld' SSID. In any case, the configuration requires that quality of service (QoS) capabilities be enabled on both the network and the voice clients.



The diagram above shows the functional entities required for secure UMA service over a corporate WLAN.

- The phone must be configured to look for the appropriate corporate WLAN SSID;
- The phone first associates and authenticates to the enterprise WLAN, in the same way as a PC. This will normally use some form of RADIUS-based WPA2/802.1x method such as EAP/PEAP. Configuring a phone for this is a technically sophisticated task, as it may need certificate information to recognize the corporate network, and some credentials and options must be configured. Each phone must be configured in this way, but only once;
- WPA2 requires the device to authenticate with a password whenever it connects to the WLAN, a procedure with which corporate PC users are familiar. WPA2-capable UMA phones follow the same regime, but to simplify connections, it is possible as an option to pre-configure the password on the phone rather than require the user to key in the password every time they enter Wi-Fi coverage. If such a phone is lost or stolen, it will continue to receive service until it is deactivated or blacklisted on the corporate WLAN or RADIUS server – and, of course, it will have mobile network service until the operator is informed. However, because 802.1x allows individual passwords rather than pre-shared keys as in the previous model, a single compromised password does not affect other users of the network;
- Following this the phone uses DHCP to lease a corporate IP address;
- The phone must now traverse the corporate firewall and NAT. There are two options: either the firewall can allow all corporate-initiated flows unconditionally, or ‘pinholes’ must be opened for UMA service. If the latter option is chosen, different rules must be written for each supported UMA carrier. As noted elsewhere, the specific requirements are for ISAKMP/IKE and IPsec, assuming DNS is already enabled. Firewall rules could for instance restrict IPsec flows to only ‘well-known’ UMA UNC IP addresses.

The newest business-oriented UMA mobile phone models support WPA2/802.1x. These models fully support access via the corporate LAN to the enterprise intranet.

## QoS considerations

As noted above, it is important to ensure that UMA users experience good performance on their voice calls. The key to providing priority for voice traffic over data is the wireless multimedia (WMM) feature, a certification of the Wi-Fi Alliance. Today’s enterprise-grade WLAN equipment supports WMM for QoS, where WMM recognizes the diffserv tags on frames and maps the 802.1d classes of service to four queues defined in 802.11e. An incoming frame with high priority will be mapped to the high priority queue and will be allowed preference when contending for a transmit opportunity on the wireless medium.

Most UMA phones support WMM, so the frames they transmit will be at high ‘voice’ priority. By default, this priority tagging will be respected by the Wi-Fi infrastructure and maintained throughout the network. Even though UMA uses an IPsec tunnel, phones usually apply voice priority tags to the outside of the tunnel.

---

If a phone does not use WMM, it is still possible to provide good QoS over Aruba infrastructure by writing a firewall rule to recognize UMA traffic and assigning all such traffic high priority. Such a rule might be targeted at IPSec protocols where the destination is a UNC gateway IP address. This example will cover all traffic streams except those upstream from the phone to the access point, though it has been found that priority queuing, even if only in the downstream direction, is a very effective QoS implementation.

While QoS ensures that voice traffic receives priority over data, it is possible to overload an access point when the amount of voice traffic approaches its capacity. Under these conditions, some or all the voice calls will be impacted. Call admissions control (CAC) is a feature that limits the number of calls below this threshold, typically between 12-25 active calls per access point. Most enterprise WLANs implement CAC, however, UMA traffic is carried in IPSec tunnels and WLANs may require enhancement to recognize UMA packets as voice traffic. In the absence of such an enhancement, the network manager should use network design and traffic engineering to ensure that the maximum number of simultaneous UMA calls per access point is less than the limit. A dense deployment of access points in which each access point serves only a small area, combined with a load-balancing feature, will keep the number of active calls per access point below the CAC threshold.

### **Battery life**

Recent advances in voice over Wi-Fi technology have significantly reduced concerns over reduced battery life that affected earlier dual-mode cellular/Wi-Fi phones. The key standard for long battery life is WMM-PS (power save), already supported by most enterprise WLAN infrastructure and some UMA phones. WMM-PS allows the phone to shut down its Wi-Fi radio except for the very short intervals when it is sending or receiving frames over the air. Aruba and some other enterprise WLAN vendors incorporate additional features that extend battery life and work effectively with standards-compliant clients such as UMA phones.

### **Inter-access point handover**

While residential UMA service assumes a single Wi-Fi access point, enterprise WLANs cover large buildings by deploying many access points with overlapping coverage. This means that in an enterprise deployment, a handset will hand over voice calls between access points as the user roams around the facility. Enterprise WLANs typically include features to facilitate fast, accurate inter-access point handover. Included among these is a provision for the infrastructure to maintain the same IP address as a client moves, thereby obviating the delays – and interruptions to voice calls – associated with leasing new IP addresses through DHCP.

Additionally, when using the WPA2 protocol to achieve high security, a key feature is opportunistic key caching. OKC allows centralized WLANs to significantly reduce the time required to generate new security keys, necessary when roaming between access points. This feature can reduce voice call interruptions from several hundred milliseconds to sub-fifty millisecond levels. Some UMA phones already implement OKC today, others will be coming to market soon.

### **Security Considerations**

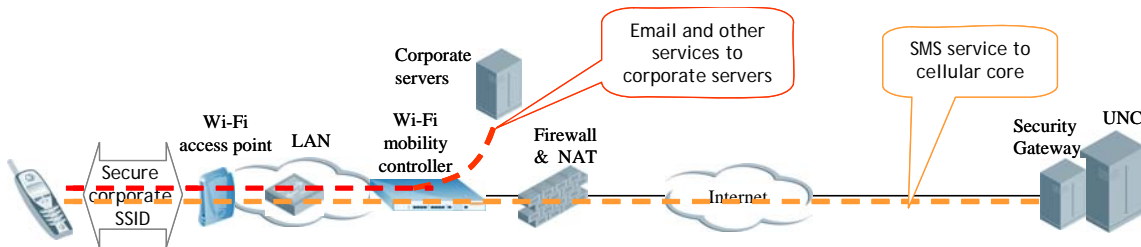
The volume of UMA traffic on the corporate WLAN will normally be so small that it will not have any adverse effect on existing voice or data traffic. Each active UMA call takes approximately 65 kbps on Ethernet or 200 kbps with 802.11 overhead: inactive UMA phones still generate traffic for registration and signaling, but the data-rate is negligible. Nevertheless, it may be prudent for the network manager to configure traffic-shaping features on the WLAN. These can target individual streams or aggregate flows. For



instance, WLAN traffic shaping could be configured to restrict IPSec traffic to a ceiling of no more than 25% of the bandwidth of any access point, ensuring that other corporate WLAN traffic is minimally impacted by the addition of UMA services.

## Mobile Data Considerations

Apart from voice calls, modern GSM phones support data services. Certain mobile data services such as SMS and MMS depend on functionality in the mobile core network, so this traffic is always directed via the UMA IPSec tunnel.



However, some UMA phones now allow for non-operator mobile data services, such as email or Web browsing, to be directed outside the UMA service tunnel and directly to servers on the corporate network or the Internet. The diagram above shows how this works. Note that the phone has one Wi-Fi association on a single SSID, but maintains two or more traffic streams.


## Checklist of applicable Wi-Fi certifications

Wi-Fi devices are built to specifications defined by the Institute of Electrical and Electronic Engineers (IEEE) 802.11 series of standards, but they are tested and certified by the Wi-Fi Alliance, which uses its own names for the various 802.11 supplements. The table below includes a description of the Wi-Fi Alliance certification programs.

Wi-Fi Alliance Certification	Notes
802.11g	802.11g allows the phone to connect at higher data rates than 802.11b: an 802.11g infrastructure with 802.11g phones allows more calls per access point than 802.11b (approximately 25 vs 12). 802.11g infrastructure is backwards-compatible with 802.11b phones.
802.11a	802.11a operates in the 5 GHz radio band, where there is less interference, but usable range is lower. When both infrastructure and phones are 802.11a-capable, performance should be better than with 802.11g in the 2.4 GHz band.
WPA2 Enterprise	Wireless Protected Access 2 uses advanced authentication and encryption techniques to provide security – WPA2 is configured for most corporate networks with PC clients. An 802.1x option such as PEAP uses rotating keys and is superior to a pre-shared key (PSK) regime, where all clients share a common password.
WMM	Wireless Multimedia is a Quality of Service certification taken from 802.11e.
WMM-PS	WMM – Power Saving is also taken from 802.11e asynchronous power save delivery (APSD). It enhances battery life.
802.11h	802.11h is useful in extending battery life, as it allows the client device to lower its radio transmit power when close to the access point it is communicating with.
802.11i OKC	Opportunistic Key Caching is an option in 802.11i (the authentication and encryption standard) that enables fast, secure inter-access point handovers.

An example of the Wi-Fi Alliance certification Web page ([www.wi-fi.org](http://www.wi-fi.org)) is shown below, in this case for the BlackBerry Curve 8320. This Web site is available to the public and offers an opportunity to easily verify the capabilities of Wi-Fi devices.

**Wi-Fi® Interoperability Certificate** Certification ID: WFA5355

 This certificate indicates the capabilities and features that successfully completed interoperability testing by the Wi-Fi Alliance. You may find detailed descriptions of these features at [www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php).

**Certificate Date:** August 23, 2007  
**Category:** Smartphone, dual-mode (Wi-Fi and cellular)  
**Company:** Research in Motion Limited  
**Product:** BlackBerry 8320 Smartphone

**This product has passed Wi-Fi certification testing for the following standards:**

IEEE Standard	Security	Multimedia	Special Features
802.11b 802.11g	WPA™ - Personal WPA™ - Enterprise WPA2™ - Personal WPA2™ - Enterprise  <b>EAP Type(s)</b> EAP-TLS EAP-TTLS/MSCHAPv2 PEAPv0/EAP-MSCHAPv2 PEAPv1/EAP-GTC EAP-SIM	WMM® WMM Power Save	Wi-Fi Protected Setup™ PIN

For more information: [www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php)

## Benefits of UMA service to the enterprise

Enterprises will typically adopt UMA for two primary reasons, improved coverage and reduced costs. The coverage aspect is straightforward, because a corporation can set up Wi-Fi access points in areas with poor cellular coverage to overcome gaps in coverage and call dropouts. Indeed, with state-of-the-art, centrally-managed enterprise WLANs, a global configuration change can allow Wi-Fi UMA access from any company location.

A proper analysis of cost savings depends on the UMA carrier's tariffs, the cost of alternative communications methods that might be used, and the calling patterns of corporate users. Whenever the phone is connected to the UNC over Wi-Fi, that path will be used in preference to GSM for both outgoing and inbound calls.

---

Consider for example the T-Mobile HotSpot @ Home service. Calls can be made over home Wi-Fi routers, corporate networks, if enabled, and from T-Mobile public hotspots in locations such as commercial restaurants, shops and airline lounges. It is also possible to connect to any open Wi-Fi hotspot, but the phone must be configured for the individual SSID of that hotspot.

### **Saving costs with smaller air-time plans**

Cellular service in the US is sold as buckets of air time, where the total number of minutes on-call per month is capped, with penalty rates for 'overage.' With the HotSpot @ Home service, all calls over Wi-Fi are excluded from this calculation. This translates into savings for the user if a smaller air-time package is chosen. For example, a consumer might be able to move from a 1000-minute/month plan to 600 minutes/month if approximately 50% of their calls were made over Wi-Fi, saving \$10/month. A business user might be able to move from 2500 to 1500 minutes/month, saving \$40/month.

### **Saving costs with less fixed-line calling**

As employees use their mobile phones for increased calling over Wi-Fi, there is a natural decrease in the minutes used on the fixed network. Calling via the enterprise PBX typically costs \$0.02-\$0.40/minute, so migrating these minutes to an unlimited mobile calling plan results in cost savings.

For telecommuters or work-at-home employees, the savings can be even greater. Many remote employees purchase both fixed line voice service (often a VoIP service) as well as a broadband connection and mobile service. With HotSpot @ Home, the employee can replace the cost of the fixed line VoIP service, because voice calling is included as part of the plan.

Aruba's Remote Access Point solution is optimized for remote offices and is already used to extend corporate Wi-Fi data services securely to the home. Once installed, it allows UMA mobile phones to access enterprise services subject to the same security that is enforced at the corporate facility. An additional benefit is that the mobile phone does not need any special reconfiguration for use in the home office.

### **Saving costs on international roaming**

US service plans all include unlimited national calls, but international calls are charged per-call, with various plans available for volume callers. HotSpot @ Home service does not distinguish between Wi-Fi and cellular when international calls are originated – the charges will be the identical. However, when the user is travelling, calls made over Wi-Fi will be charged as if the call was placed over Wi-Fi in the U.S.

For example, a business user based in the U.S. and calling France would pay the T-Mobile rate for the call whether connecting from a home Wi-Fi router or over the mobile network. However that user, when traveling in France and calling the US would not incur any calling charges when using Wi-Fi as the link to T-Mobile's US UNC. Also, incoming calls when in France would not incur international roaming charges when the user was within Wi-Fi coverage. These represent substantial savings for many travelers, as international cellular roaming charges are often significant.

Opportunities for making calls over Wi-Fi when traveling include calling over suitable public hotspots or open access points and using a WLAN at a corporate location (configured for UMA service). Also, travelers with a pre-configured corporate access point, such as Aruba's Remote Access Point, can connect to any Internet connection, such as a hotel or home Internet connection, and provide UMA-capable corporate WLAN coverage on the road. UMA calls over all such services will tunnel over the Internet to the UMA operator's home UNC.

---

## **Saving costs on data services**

Data services are important to many business users. With some UMA phones, all data streams take the IPSec tunnel to the UNC, and with the T-Mobile HotSpot @ Home service, these are billed at the same rate as the cellular data services. In this case there is no cost advantage to using Wi-Fi, although data speeds and performance may be better. UMA service plans differ between mobile operators and some operators may charge a lower rate than T-Mobile for data usage on Wi-Fi.

With some UMA phones, it is possible for the phone to bypass the UMA tunnel over Wi-Fi for non-operator services such as Internet browsing. In this case, not only should performance be improved, but the data will not be metered by the carrier. Note, however, that the cost savings may not be significant when the user has an 'unlimited' data plan.

Other opportunities for cost savings include using data services such as email and Web access when operating within Wi-Fi range, and switching off data services when travelling internationally (except when on Wi-Fi), because international data services can result in unexpected service charges.

As more enterprise data services are enhanced for mobile access, UMA may offer security as well as performance advantages when operated on Wi-Fi in preference to cellular. Some of these applications are very sensitive to bandwidth and latency, and performance should be significantly better over corporate Wi-Fi networks than using cellular access.

## **Cost of the phone and UMA service**

The evidence to date is that UMA phones are priced at the same level as equivalent cellular phones. At the time of writing, T-Mobile prices the Samsung T409 and Nokia 6086 at \$49.99 (with a service commitment), and the BlackBerry Curve is \$249.99, while the equivalent without Wi-Fi is \$199.99 from AT&T and \$299.99 from Verizon Wireless.

In the case of T-Mobile, HotSpot @ Home service is priced at \$19.99/month for unlimited calling when on Wi-Fi. T-Mobile offers a home Wi-Fi router for \$49.99, but phones can be configured to use an existing home router.

The tables below show pricing model examples, and assess the potential cost benefits that can be realized by different enterprise users when moving to UMA.

Office-Based User (works from office and/or home with a Wi-Fi router at both locations)				
	Cost before UMA	Cost with UMA	Cost savings	Notes
Cost of the phone (Samsung T409)	\$49.99	\$49.99	0	Voice-oriented phone, no strong data features
Calling plan	\$49.99	\$39.99	\$10.00	Per month, moving from a 1000 to a 600-minute plan (or 600 to 300 minutes)
HotSpot @ Home service	0	\$19.99	(\$19.99)	
Reduced fixed line calling (500 min @ \$0.03/min)	\$15.00	\$0	\$15.00	Calls made on mobile phone are part of unlimited long-distance package, rather than per-minute via the corporate PBX
Total monthly savings per user			\$5.01	

Home-Based Teleworker				
	Cost before UMA	Cost with UMA	Cost savings	Notes
Cost of the phone (Samsung T409)	\$49.99	\$49.99	0	Voice-oriented phone, no strong data features
Calling plan	\$49.99	\$39.99	\$10.00	Per month, moving from a 1000 to a 600-minute plan (or 600 to 300 minutes)
HotSpot @ Home service	0	\$19.99	(\$19.99)	
Home office telephone service (e.g. Vonage)	\$25.00	\$0	\$25.00	Calls made on mobile phone are part of unlimited long-distance package, not charged per-minute
Total monthly savings per user			\$15.01	

Road-Warrior User (significant data and international travel)				
	Cost before UMA	Cost with UMA	Cost savings	Notes
Cost of the phone (BlackBerry curve)	\$249.99	\$249.99	0	PDA with email, PIM, Web service
Calling plan	\$89.99	\$69.99	\$20	Unlimited data, 1500 -> 1000 minute/mo plans. These plans include BlackBerry Enterprise Server connection for push email from corporate servers
HotSpot @ Home service	0	\$19.99	(\$19.99)	
International calling	\$50.00	\$15.00	\$35.00	Depends on travel patterns
Total monthly savings per user			\$35.01	

---

## Conclusion: opportunities for UMA service in enterprises

Although UMA service was developed with the consumer and residential service in mind, it has immediate applicability to businesses. In this paper, we identified and quantified the main benefits to employees associated with using UMA service:

### Reliable coverage

Providing reliable coverage in the office is as important for a business as home coverage is for the consumer. For a modest investment in Wi-Fi infrastructure and Internet connectivity – which most businesses already have to some degree – it is possible to compensate for poor cellular coverage and enable the reliable use of cellphones at work.

### Cost savings

The tariff for the T-Mobile HotSpot @ Home, probably typical of UMA services, means that the extra cellphone usage in the office will not result in higher expenses to the individual or the organization. In fact, it should be possible to reduce voice service costs by moving to a smaller bucket of minutes. This will depend on the number of calls made from Wi-Fi locations. In addition, users who travel internationally will be able to realize considerable cost savings when making (or receiving) calls over Wi-Fi rather than cellular. While most ‘road warriors’ already have ‘unlimited’ data plans, and so would not save costs by using Wi-Fi connections for email and Web access, except when roaming internationally, the performance of these services should be considerably better when in Wi-Fi if the phone can support a direct Internet connection in addition to the UMA tunnel to the UNC.

There are several steps a network manager should take to enable UMA service on the corporate WLAN, and various levels of support that may be appropriate.

- The corporate LAN must be protected and kept secure. To this end, the UMA traffic should either be kept separate, and delivered outside the corporate firewall, or the phone must be subject to the same security requirements that corporate PCs must meet for Wi-Fi authentication;
- In the first case, it is difficult to distinguish between corporate HotSpot @ Home users and public users ‘off the street.’ To highlight this distinction, this note analyzed both ‘public’ access and a second option where a weak authentication method such as WPA PSK identifies corporate UMA phones, denying service to others. It will be necessary to modify the guest access SSID or add a new one in order to implement either of these models, but both provide good security when implemented on an Aruba WLAN;
- In the third model, the phone must offer appropriate authentication/encryption capabilities, probably WPA2/802.1x, and will require individual configuration to access the WLAN, similar to a PC. Again, it is important to implement appropriate firewall rules, either on the Aruba equipment itself or on the main corporate firewall.
- Another alternative is to enforce a policy of denying access to UMA service, a goal that can be achieved through the integral firewall of an Aruba WLAN;
- Quality of service can be assured through the WMM protocol, while other aspects such as bandwidth-hogging can be controlled by bandwidth contracts enforced by the WLAN.

---

The HotSpot @ Home service offers wider benefits for businesses willing to challenge traditional assumptions. Since it is possible to provide assured coverage for mobile phones at no additional cost, some small businesses will be able to offer employees UMA phones as their sole voice communications tool – substituting for desk phones – while the email capabilities of devices such as the BlackBerry may mean fewer PCs are required. Whatever the degree of adoption, UMA-based Fixed-Mobile Convergence can be a very useful and cost-effective tool for both businesses and consumers.

## **About Aruba Networks, Inc.**

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of mission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. 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 <http://www.arubanetworks.com>.

*© 2008 Aruba Networks, Inc. All rights reserved. Aruba Networks, BlueScanner and RFprotect are trademarks of Aruba Networks, Inc. All other trademarks or registered trademarks are the property of their respective holders. Specifications are subject to change without notice.*

WP\_FMCUMA\_US\_080110

