ARUBA™
The Mobile Edge Company

Technical Brief

The Mobile Edge – An Architecture for Mobility, Security & Convergence in Enterprise Networks

Jon Green
Product Marketing Manager

The Mobile Edge – An Architecture for Mobility, Security & Convergence in Enterprise Networks

Introduction

A recent survey of IT managers identified the top three technology trends impacting their departments as mobility, security, and convergence. Mobility, strongly demanded by users, delivers a competitive advantage by providing instant access to information anytime and anywhere a user needs it. Security relates to the confidentiality, integrity, and availability of information, and has quickly become a business imperative with regulatory implications. Finally, converged voice and data communications over a single network promises lower costs coupled with a richer experience for end users with converged applications.

These trends, seemingly independent, intersect at the edge of the enterprise network where users and devices plug in to gain access to network services. Today's 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 must be applied to ports in order to protect the network from unauthorized users and devices. Convergence requires that these ports deliver Voice over IP (VoIP) services and Power over Ethernet (POE) in order to power desktop VoIP phones. Mobility involves the connection of wireless access points to the network and the extension of the network through WANs and VPNs. However, mobility breaks the fixed edge concept of port-based networking. Since users are mobile, they can connect to any port at any time. In the context of a fixed edge, mobility merely means taking the existing network port and making it wireless. True mobility requires the network to support seamless user roaming anywhere the user moves.

Given that today's fixed edge does not support any of these functions, it is only natural to conclude that the fixed edge ports need to be upgraded in order to meet the demands of security, mobility and convergence. This is a daunting task for network managers who have already built a reliable and stable network that performs predictably for mission-critical enterprise applications. Major upgrades to the fixed edge are not only very costly but also very disruptive. Ultimately, they are also not necessary.

There is another solution that can deliver all these advanced capabilities without requiring massive upgrades to the entire network. The irreversible trend towards mobility is giving birth to a new kind of edge – the 'mobile edge'. The mobile edge allows users and devices to connect over the air and across any network, to securely gain access to enterprise resources. It is a new layer in the network that logically sits on top of existing fixed networks and fulfills the requirements of security, mobility and convergence without requiring major upgrades to the existing network. The mobile edge is architected to securely work over existing IP network facilities, and extends across both private enterprise networks as well as the public Internet.

The mobile edge by definition supports true mobility where users can seamlessly and securely roam across multiple locations. In addition, it delivers convergence through converged mobile devices and Voice over Wireless LAN (VoWLAN) handsets. This eliminates the significant expense of adding powered VoIP ports to the fixed edge. Further, the mobile edge is built on the notion of identity-based

security. Since users can roam across multiple ports on a network, port-based security models do not apply to the mobile edge. Identity-based security is far more granular than port-based security since it applies policies at the user and device level. The mobile edge extends these granular identity-based security services to the fixed edge in order to protect the overall enterprise network from unauthorized users and devices with a single wired/wireless security architecture.

The 'mobile edge' not only solves today's challenges around mobility, security and convergence but provides a roadmap to reduce overall costs of the network infrastructure. The ultimate goal of the 'mobile edge' is to radically transform enterprise network economics by eliminating the costs of cabling infrastructure and the operational expense of moves, adds and changes. This introduces a dilemma for incumbent networking vendors. The incumbent vendors, in order to continue their growth, must entice customers to spend more on their networks. The 'mobile edge', by drastically reducing networking costs, runs directly counter to the needs of the incumbent vendors. The 'incumbent's dilemma' develops whenever major turning points in technology develop – the incumbent cannot grow business by offering a solution that allows customer to spend less.

The 'mobile edge' is not based on this incumbent's dilemma. It is an evolutionary new architecture that delivers mobility, security and convergence for today's networks and builds on a vision where the enterprise network will ultimately have far fewer ports than today.

Mobility, Security and Convergence at the Fixed Edge

At the fixed edge are an average of three physical ports – one for voice and two for data. Feeding those ports is a voice PBX sitting in a server room and Ethernet switches with high port density in the wiring closets. Voice ports are tied to a specific telephone number, and a specific user is expected to answer that number when it is called.

These separate voice and data networks are not designed for mobility. To add mobility, many enterprises have looked into wireless LANs. However, many networking vendors treat wireless as yet another data link – nothing more than a way to extend the wired network into the realm of radios. This is a shortsighted view of wireless, and leads to disruption and another cycle of upgrades. At the same time, such an approach ignores the fact that mobility extends outside the walls of the enterprise facility – users need connectivity at remote offices, at home, and while on the road.

There are also approaches to providing security in the fixed network. The primary focus has been on authenticating devices and users with 802.1x. This protocol puts all wired switch ports in a "blocking" state until a user has successfully provided authentication credentials. But implementing 802.1x in the wired network is not an easy task. First, it often involves upgrading wiring closet switches to new hardware. At a minimum, it involves software upgrades and the installation of an authentication server. Finally, activation of 802.1x requires that the switch and client device enable it at the same time – and only after the client has been configured. Beyond implementation difficulties, 802.1x in the wired

network has a number of inherent limitations that make it less than ideal for truly securing the network. Most of the security provided by 802.1x involves placing a port into a specific VLAN – but VLANs were never designed to be used as a security control. Adding wireless to a fixed network complicates the situation even further.

To deal with convergence on the fixed edge, many enterprises are moving to Voice over IP (VoIP) to consolidate multiple services onto a single converged network. Traditional fixed networks do not realize the full potential of convergence, however, and impose significant cost and disruption to deploy. Fixed networks must be upgraded to provide power over Ethernet (PoE) to desktop handsets. To support PoE, additional power in the wiring closet is required, battery backups must be provided for emergencies, and additional cooling capacity must be added to the closet to deal with excess heat produced by the PoE equipment.

Even after migrating to VoIP, network managers often find that users do not actually use the expensive voice networks they have installed. Instead, an increasing number of users provide their mobile phone number to business contacts so that they can be reached when not at their desks. These employees then bill their employer for the cost of the mobile phone, since they are used for business. Cellular phones do not provide the voice quality of a wired desktop phone, but the convenience of mobility outweighs any possible quality concerns.

Leveraging the Irreversible Trend Toward Mobility

User Demand for Mobility

Mobility is a trend that has been gaining momentum since the first laptop computer was sold. People move around, and once people began doing their jobs with the help of equipment such as computers and telephones, they have wanted the equipment to move too. Laptop computers and PDAs gave users data mobility, but network connectivity then became a problem as the network became a more critical enterprise resource. Cordless phones provided voice mobility in people's homes, but were unsuitable for enterprise use. Cellular phones solved the mobility requirement, but were too expensive for an enterprise to provide to their entire employee base. Still, demand for mobility has driven many employees to use their cellular phone as their primary telephone, only using their desktop phone occasionally. Many people consider voice mobility to be solved – but those who pay the bills remain unsatisfied.

A solution for data mobility evolved in the mid-1990s in the form of wireless LANs. Originally developed for enterprise applications, wireless LANS were largely rejected by the enterprise after serious security flaws were exposed in the technology. Wireless vendors responded with new security protocols that fixed these problems, but in the meantime wireless LANs found a new market – in the home and in public Internet hotspots. With easy-to-install broadband routers with integrated wireless costing less

than US$100, wireless deployments in homes skyrocketed, driving laptop manufacturers, PDA manufacturers, and even Intel to integrate wireless into their products. Finding wireless LAN equipment inexpensive and easy to use, some employees began bringing this technology into the enterprise and connecting it to the network, introducing major security holes into the network. No amount of corporate policy writing, IT radio sweeps, and threats of firing seems to keep "rogue" APs out of the enterprise network. The user demand for mobility is too strong.

Business Demand for Mobility

Users are not the only driver of mobility demand. Businesses in particular industries also demand mobility in order to achieve competitive advantages. In businesses with warehouses, wireless is critical for inventory tracking, order processing, and movement of goods. Often, specialized equipment such as ruggedized handheld computers and barcode scanners are used in these locations to connect the user instantly with warehouse databases and application servers. In retail environments, mobile point of sale equipment can be used to set up checkout locations anywhere, even outdoors, at a moment's notice. The same handheld barcode scanners used in warehousing are also used in retail for inventory management.

In health care, hospitals use wireless to enhance patient care and to reduce personnel expenses. Some hospitals have equipped doctors with tablet PCs that are wirelessly connected. These tablet PCs let a doctor instantly pull up any and all data on a patient without having to leave the bedside. Through the wireless LAN, a doctor can order tests, send notes with patient records as attachments to other doctors, and even change settings on patient care equipment. The implementation of wireless technology in health care reduces expenses, reduces errors, and increases patient and provider satisfaction.

Colleges and universities must now offer wireless LANs in order to compete for the best students. College students today have grown up with wireless technology, from cellular phones to wireless LANs. Students today are also avid Internet users, with instant messaging and email topping the list of applications used. Demand for mobile Internet access is so strong that colleges that do not provide such access are at a disadvantage when recruiting students.

Economics of Mobility

IT managers and financial analysts have both begun to calculate the cost savings possible with mobile networks. One large financial institution calculated that if a WLAN connection were able to increase employee productivity by just one hour per week, an average annual productivity enhancement of nearly $900 per employee was possible. Subtracting out the cost of the wireless LAN equipment, net savings per year fell just under $800 per employee. Clearly, productivity is one area where wireless LANs can impact the bottom line.

Productivity, however, is hard to quantify. What really excites financial analysts is the prospect of buildings that are all-wireless, without the need for cabling. In a pure wireless voice and data

environment, cable does not need to be pulled, wiring closets do not need Ethernet switches, power does not need to be provided to closet switches, maintenance contracts do not need to be purchased on wiring closet equipment, and employees moves, adds, and changes cost nothing. Technology is rapidly advancing to the point where all this is possible.

Mobility Enables New Applications

The most exciting driver of mobility is what comes next. Wireless applications today are primarily outgrowths of wired technology. For example, wireless inventory tracking permits real-time database updates and queries, but the same process can be performed using batch updates when a handheld device is placed into a docking cradle. And for the general enterprise user, the wireless LAN is simply a productivity-enhancing tool. It may be more efficient to answer a question immediately while in a meeting, but the same question could still be answered back at the user's desk with a follow-up email.

True mobile applications are enabled by the mobile network, and cannot function without it. These mobile applications are only just now in the design stages, since they require that the mobile network is in place first. Location services - the ability to find the physical location of a wireless device inside a facility - is one example of a true mobile application. Some enterprises are beginning to use location services for asset management, placing small Wi-Fi "asset tags" on expensive pieces of mobile equipment so that it can be tracked. Sports arenas have successfully used this concept with plasma television screens on wheels, and also with small electric carts used to transport people and supplies around the arena. Hospitals have used wireless asset tracking to keep track of mobile carts, wheelchairs, and hospital staff. Other examples of mobile applications include social networking devices, RFID, and applications that use physical proximity of one or more objects as an input to business logic. Mobile applications will develop into competitive differentiators for their users, and those who do not adopt them will be left behind.

The Mobile Edge Architecture – A New Approach

Today, the fixed edge is giving way to a new "mobile edge" – a new way of connecting users to information. The mobile edge transcends the enterprise network perimeter, appearing wherever the user needs access to information – in the central office, in a regional or branch office, at retail outlets, at home, and on the road. The mobile edge embraces mobility, security, and convergence, solving the problems of all three areas simultaneously while delivering dramatic economic savings over traditional fixed networks.

The mobile edge uses wireless networks, both for voice and data, wherever wireless can be used. Inside enterprise facilities, high-performance and highly-reliable wireless LANs are deployed to provide dense coverage. In homes, hotel rooms, other companies, and wherever Internet-connected Ethernet ports are available, portable wireless access points provide secure connectivity back to the nearest enterprise facility. Finally, at public wireless hotspots, client software provides a secure link to the nearest mobile edge location.

The mobile edge is an overlay network consisting of both hardware and software. It makes use of existing high-speed networks – the enterprise LAN, the enterprise WAN, and the Internet. The mobile edge does not replace these existing networks, but deploys on top of them as a service overlay, preventing disruptive equipment changes and preserving existing investment. Most enterprise networks have been engineered for high performance and high reliability – many have multi-gigabit backbones, dual redundant fiber to each wiring closet, and hot-standby datacenters. There is no need to change these networks to add mobility, security, and convergence. Instead, these three additions can be delivered as network services through the mobile edge. In addition, these services can be implemented in a phased approach, avoiding the disruption of large-scale cutovers.

The mobile edge delivers three primary benefits:

- Freedom of access to information
- Identity-based security
- Dramatically transformed network economics

Freedom of Access to Information

The mobile edge provides freedom of access to enterprise voice and data networks wherever the user travels – in the office, at home, and on the road. It does so while satisfying user demand for wireless and mobility. The user is not necessarily "always connected," but has the option to be connected when desired. This is a compelling competitive advantage to a business, since employees with better access to real-time information are much more able to make good decisions. One well-known financial services firm has instituted a policy that all "non-study" questions asked during meetings must be answered before the meeting ends. In the past, meeting participants would have to return to their desks to find answers or call for outside assistance. After implementing wireless, these meeting participants can open their laptops, find an answer, and report it immediately. The increased decision-making power available through deploying wireless gives this firm an advantage over competitors and helps it operate more efficiently.

The trend in fixed networking over the past decade has been one of increasing speed. Today, fixed networking vendors are trying to move these networks to switched 1000Mbps to the desktop, but there is little user demand for these expensive upgrades. Studies show that the average desktop user consumes no more than 2Mbps on average, with only occasional bursts above that. What users are demanding is mobility: faster and more convenient access to information. Wireless LANs provide a similar benefit to cellular phones. Users accept lower voice quality on cellular phones because the benefit of mobility outweighs the loss of quality. Similarly in wireless LANs, users are willing to give up some of the performance of the wired LAN in exchange for the benefit of mobility. In both cellular telephony and wireless LANs, advances in technology are quickly erasing any performance differences between their wired counterparts so that eventually, users will have both performance and mobility.

Identity-based Security

The mobile edge drastically improves network security by eliminating excess privilege on the network while providing identity-based auditing. 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 joins the network. Once this identity is known, custom security policies may be applied to the network so that only access appropriate to the business needs of the user or device is provided.

Identity is learned through the authentication process, during which the device or the user provides some type of identifier, normally a username. Once identity is learned, it is mapped to the business role of that user or device. The business role may be determined through membership in specific departments or groups, security clearance, or the actual business position of a user. Role information is normally contained in the enterprise authentication system, such as Active Directory in a Microsoft Windows environment. Some examples of roles and their associated security requirements include:

- A member of the sales department, who needs access to the Internet and to internal web-based sales databases. A member of the sales department has no business need to communicate with servers in the human resources department.
- An outside visitor, who needs only access to specific applications on the Internet only during daytime business hours.
- A POS (Point of Sale) handheld device in a retail environment that must send credit card data as well as download inventory and price updates. This device would communicate only with a specific server using specific protocols.
- A public PC-based kiosk for use by the general public. This device would be permitted to do web browsing, but would be denied all other network access.

Dramatic Economic Advantages

The mobile edge transforms network economics by radically reducing costs. As networks become mobile, wires are gradually eliminated. This translates directly into reduced cabling, reduced switching equipment, and the elimination of move/add/change costs.

In a traditional wired network, there is an average of three Cat5 cables run to every work location. Installing this cable and terminating jacks is a huge expense. In the wiring closet, these cables must be connected to Ethernet switches. Each port carries with it a cost in capital expense, in ongoing maintenance and support, and in power draw. Networking vendors have done a poor job maintaining investment protection in this equipment, often allowing only the sheet metal of the chassis itself to remain when an upgrade in performance or features is needed. Finally, when employee work locations move or change in the fixed network, new cabling must often be run and switch ports reconfigured.

Wireless, on the other hand, permits five to ten users to share a single wired port where the AP is connected. The only cabling required is to connect the APs back to a much smaller wired network. If

one hundred ports were required in the wiring closet to support the fixed edge, only ten ports are needed to support the mobile edge. Moves, adds, and changes are a non-event in a wireless network, since users and devices are always assumed to be moving.

In many enterprises today, wireless has become the primary connection to the network for the majority of users. The wired network is still there, used by high-bandwidth users and as a backup to the wireless. This did not happen because IT managers made it happen – users instead realized on their own that the wireless network satisfied all their requirements, and began to use it. As wireless technology continues to mature and advance, both in terms of performance and reliability, wireless will eventually become the exclusive connection to the network, and the wired edge will cease to exist. Once this happens, wireless can provide a ten-to-one cost advantage over traditional wired networks, all while delivering the mobility demanded by users and solving issues with security and convergence.

Many networking vendors will talk about one or more aspects of the mobile edge, but few can deliver it in a cost-effective manner. It is the economic benefit of the mobile edge that explains why incumbent fixed-edge providers cannot offer such a solution, and that answers the question, "Why not integrate the wired and wireless network?" The mobile edge offers a ten-to-one cost advantage over fixed networks. In order to survive, incumbent providers must entice customers to increase expenditures, not reduce them by ninety percent. These vendors will provide wireless, but will do so in a way that makes wireless just an extension of the wired network – requiring upgrades, replacement, and continued reliance on a single vendor.

Capabilities Required at the Mobile Edge

Properly implementing the mobile edge requires a number of considerations. At a high level, the mobile edge must deliver mobility, security and convergence. It must do so in a way that is cost-effective in terms of equipment costs, installation costs, and ongoing maintenance costs. It must not require additional people to manage, and must provide self-management and self-troubleshooting. Finally, if the economic advantages of the mobile edge are to be realized, the mobile edge must be reliable enough that users will accept it as their exclusive means of connection.

More specifically, the mobile edge must deliver the following:

1. **Identity-based security to protect the network and mobile users**

   The mobile edge is, by definition, mobile. On the mobile edge any user can appear in any place at any time, so the network must recognize the user or device by identity. Identity-based security solves security problems by applying rules to people rather than to ports on the network, only permitting access appropriate to the business role of the user.

2. **Non-disruptive integration into existing networks**

   The mobile edge must be cost-effective in order to enjoy widespread adoption. Deployment of the mobile edge cannot force large scale upgrades or changes to the existing infrastructure, nor can it

force network downtime. The mobile edge must integrate into existing management tools, security monitoring systems, and auditing procedures.

3. Secure convergence for mobile VoIP and data services

The mobile edge must be multi-service. On the mobile edge, voice is a critical service. Voice over wireless LAN (VoWLAN) provides all the mobility benefits of cellular with the cost savings of VoIP and does not require expensive power upgrades to wiring closets. Newer dual-mode voice handsets operate over the enterprise wireless LAN wherever it is available, and over the public cellular network everywhere else, providing true cost-effective voice mobility to users.

4. Adaptive radio management for self-configuring WLANs

The mobile edge requires adaptive control of the air. Radio frequency (RF) transmission is an inherent part of wireless, and one with which many network administrators are not familiar. The goal of any wireless deployment is to provide the required coverage while guaranteeing maximum performance. With the pervasive nature of wireless on the mobile edge, RF tuning cannot be a manual task that the network administrator must perform. RF management must be entirely automatic, reliable, and adaptable.

5. Remote extensions for instant enterprise hotspots

The mobile edge moves with the user. Users move outside the walls of the enterprise facility, yet still need access to enterprise voice and data networks. Left to their own devices, users will create their own version of the mobile edge wherever they need to – using DSL or cable connections at home, using open wireless networks at public hotspots, plugging into Ethernet jacks in hotel rooms, or connecting over public wireless networks such as GSM or EVDO. To avoid the support and security problems caused by this approach, the mobile edge must extend on-demand enterprise voice & data connectivity over the Internet to create secure personal hotspots wherever users need to work. These hotspots move with the user, but control and configuration remains with the network administrator.

6. Enterprise-grade scalability, reliability & performance

The mobile edge must be dependable. To realize the full benefits of the mobile edge, it must provide predictable, consistent performance and high reliability. The system should gracefully recover from all component failures with no network outage noticeable to the user. Performance should meet all requirements of mobile applications, and should remain high even in challenging RF environments. Finally, the mobile edge should grow with the enterprise without requiring additional people to manage it.

7. Open mobility platform for application development and integration

The mobile edge is a business-enabler. New mobile applications will create business opportunities and enhance existing ones, creating competitive advantages for users of the technology. Applications such as voice, location tracking, and sensor networks are the first purely mobile

applications and more are being developed as mobile networks become more prevalent. In addition to mobile applications, new services are continually being developed for security, such as network-based spyware blocking, and convergence, such as fixed-mobile handoff and emergency call location tracking. The mobile edge must be flexible, extensible, and open to application development by best-of-breed vendors.

Evolving to the Mobile Edge

Migrating from today's fixed edge to the mobile edge is not difficult, and can be rolled out in logical stages. The key to a mobile edge deployment is to look ahead – the first stage may be small and limited, but the ultimate goal is total mobility. There are seven general steps to deploying the mobile edge. While these steps may be taken all at the same time, a reasonable goal for deployment in a medium to large enterprise is approximately two to four years.

Lock the Air

The first step in any wireless deployment is to get control of the wireless that is already there. This may mean existing enterprise access points, wireless-enabled client devices, and especially rogue APs. Rogue APs – access points that are installed by the users but are not under the control of IT – are incredibly dangerous to an organization because they allow outsiders to bypass network security mechanisms and obtain direct access to an internal network. Wireless-enabled client devices are also a problem when not controlled, because they can inadvertently be used as an entry point to the internal network. Wireless bans are not a solution to the problem because they are very difficult to enforce enterprise-wide. The solution to the problem is a wireless intrusion detection system.

A wireless intrusion detection system (WIDS) can be deployed using a small number of sensors placed throughout a building. These sensors continuously scan the air and the wired network looking for rogue APs, unauthorized wireless devices, and misconfigured devices. When these threats are found, the WIDS automatically blocks them while notifying the network administrator. WIDS sensors can be deployed at remote sites also, connected over the Internet or over existing WAN or VPN connections. A key requirement of a WIDS is that it be flexible enough to start as only a WIDS and then grow to support the full mobile edge.

Wired and Wireless for Conference Rooms

Most of the early demand for wireless is for access in conference rooms, both for employees and for visitors. Using only a small number of access points, a wireless network can be built to cover conference rooms in main buildings. This wireless network provides only Internet access, only during working hours, and with policies that restrict access to specific services to prevent abuse. Employees who want internal network access over this wireless network can use their existing VPN software, just as though they were outside the office. Because wired Ethernet ports in conference rooms, visitor cubicles, lobbies, and other public areas represent a security threat, these ports can also be secured by connecting them through the same access control system that services the wireless network. Visitors

without wireless are then free to plug into these protected ports for Internet access, and employees can do the same using VPN software.

Headquarters Wireless Deployment

Wireless deployments in conference rooms relieve some of the greatest demand for wireless while giving the IT staff time to learn the technology, test authentication and encryption schemes, and research client integration issues such as wireless card driver software. Once these issues have been given proper time, a full wireless rollout in the major enterprise facilities, such as a corporate headquarters, can begin. This deployment is simply an extension of the conference room deployment, and can be done floor-by-floor by placing wireless access points around the building. APs should be placed densely, planned for small coverage cells and high performance. Given the RF management capabilities of today's wireless products, there is no need to place access points above ceiling tiles as was done in the past. Instead, APs should be placed in user space – on walls, under desks, and inside cubicle furniture. APs should re-use existing cabling and existing data networks for their connection.

Concurrent with the installation of wireless, a pilot project should be started with a small number of users. These users would no longer use VPN software to access the network, but would be configured with a strong security scheme such as WPA2. The pilot project provides an opportunity to work out any problems in the deployment, and gives help desk staff time to learn about the workings of the wireless network.

Once the AP deployment is completed and the pilot project has run to satisfactory completion, a full rollout can begin. This rollout may address only users with laptop computers, or could also include those with desktop computers as well.

Mobile Edge Extension for Telecommuters and Travelers

Once a full rollout of wireless is underway in major facilities, employees based out of those facilities who work at home frequently or travel can be provided with remote-capable access points. These remote APs connect across the Internet back to a central site, and bring up the same wireless environment as the employee would experience while in the main office. These APs can be connected to DSL lines, cable modems, NAT routers, hotel room Ethernet ports, and anywhere else that an Internet-connected Ethernet port is available. Although the enterprise wireless network has been extended far outside the walls of the enterprise facility, the network is still secure – any security used at the central site is extended to the remote site. When employees travel to branch offices, they can bring the central office wireless with them. No reconfiguration of laptops or PDAs is required when using remote APs, and no VPN software is required either. All an employee needs to do is connect the remote AP, power up a laptop, and begin using the enterprise network immediately after successful authentication.

Branch Office Wireless Deployment

Once the wireless network has been rolled out to a majority of employees at the main sites, rollout to branch offices can begin. There are a number of deployment options for branch offices, depending on

the size of the office. Very small offices may need only a single AP. In this case, the same remote AP used for telecommuters can be mailed to the office, with instructions to connect it to an existing business-class DSL line. This AP extends the wireless environment of the central site out to the branch office, with all control, security, and management remaining centralized.

For larger branch offices that require a multi-AP deployment, a smaller version of the central site deployment can be done. The experience gained from the central site deployment will guide this smaller rollout. Since there is often no permanent local IT support, a branch office deployment is best implemented after the main site is deployed and operational experience has been gained.

Wireless Voice

Once an enterprise-wide wireless data deployment has been completed, the next project to investigate is wireless voice. At the time of this writing, voice over WLAN (VoWLAN) is being deployed only by very early adopters, and there are not yet production-quality systems that can perform handoffs between public and private networks. That is expected to change rapidly, and by the time this step of a mobile edge deployment is reached, the situation should be quite different. The first step to a wireless voice rollout is to select an IP PBX, if one is not already in place. Any IP PBX that supports SIP (Session Initiation Protocol) is likely to have widespread compatibility with a wide variety of handsets and networks. The second step to a wireless voice rollout is to select the handset. The most utility will be gained from a dual-mode handset that supports both a public voice network like GSM, CDMA, TDMA, or FOMA, and a private voice network over wireless LAN. Handsets should be chosen based on factors such as PBX compatibility, advanced features, battery life, and comfort.

The rollout of the wireless voice network should proceed in similar fashion to the rollout of the wireless data network. A pilot project at a main site is critical to work out any problems in the deployment early. It is particularly important to find out if users prefer using wireless phones over their desktop phones – when this happens, the project can be considered a success. Once a pilot project is successful, wireless voice can be rolled out to the rest of the employees at the main site, followed by employees at branch offices. Once a full enterprise-wide deployment has been completed, employees can take both data and voice devices with them anywhere they go – at work, at home, and on the road.

Phase-Out of Fixed Edge

After sufficient experience and reliability have been gained in the wireless voice and data networks, it is time to consider decommissioning of the wired network, making wireless the exclusive means of connection. Unlike the initial rollouts of the technology, this step is best accomplished first in a branch or remote office because of the limited scope. By this time, wireless use will have become so prevalent that user should not even notice the disconnection of the wired network.

Ultimately, excess closet switching capacity can be sold off for surplus and the support and maintenance contracts cancelled. As new facilities are built or remodeled, cabling can be skipped as an installation step, except for that cabling needed to support the wireless network.

The true mobile edge has now arrived. Mobility, security, and convergence are all delivered, and users have the freedom of access to information wherever they go. All while spending less on networks than has ever been spent before.

Summary

The mobile edge is a revolutionary concept, but one that is evolutionary in deployment. The mobile edge is a new way of connecting users to information that transcends the enterprise network perimeter, appearing wherever the user needs access to information – in the corporate office, in a regional or branch office, at retail outlets, at home, and on the road. Deployed as an overlay to existing networks, the mobile edge delivers the mobility that users demand, the security needed by the business, and the converged multi-media network that realizes cost savings for the bottom line.

Multiple networking suppliers will attempt to deliver the mobile edge. But with a ten-to-one cost advantage over the fixed edge, do not expect an incumbent to provide it. The mobile edge is a long-term vision; but the road to mobility can be traveled today with benefits at every turn.

About Aruba Wireless Networks, Inc.

Aruba Wireless Networks is a fast-growing enterprise infrastructure company enabling the Mobile Edge, an evolutionary new network architecture that addresses three top concerns of IT managers—mobility, security, and convergence. The Mobile Edge extends the reach of enterprise networks, providing secure access to information and voice services anywhere a user needs them, enabling new applications, allowing organizations to compete more effectively, and bringing about dramatic economic benefits. To deliver the Mobile Edge, Aruba manufactures and markets a complete line of fixed and modular mobility controllers, wired and wireless access points, and an advanced mobility software suite. Privately-held and based in Sunnyvale, California, Aruba has operations in the United States, Europe, the Middle East, and Asia Pacific, and employs staff around the world. To learn more, visit Aruba at http://www.arubanetworks.com

10.10.mea.jg.2