



White Paper

Enterprise Wireless LANs A Multi-Vendor Approach

1 Introduction

The 802.11 Wireless LAN market is predicted to grow to approximately \$4bn during 2003, and is one of the product sectors of the IT market likely to show an appreciable growth over 2002. There are both significant business benefits and increased competitive advantages to be derived from Wireless, which is essentially just an enabling technology.

Approximately half of the 2003 Wireless LAN market is in the enterprise sector (an 'enterprise' being defined, for the purposes of this paper, as an organization with a reasonably large number of networked users, a high degree of network complexity or both). The enterprise sector, up until now, has been more reluctant to adopt this technology. SoHo (Small office, Home office) and SMB (Small and Medium Business) organizations have been more willing to adopt Wireless, partly because they inherently have the ability to react more quickly to new technologies.

The reluctance towards the deployment of Wireless LAN amongst enterprise organizations has a number of drivers, mainly a perceived, or actual, lack of security (a Q1-2003 customer survey by Madge shows that 61% of enterprise customers identify security concerns as being the primary obstacle to their adoption of Wireless LANs), cost, the inability of Wireless solutions to properly scale to very large numbers of users, the integration of the necessary services, management of the Wireless LAN, rapidly developing standards (with a fear of proprietary solution or 'single technology lock-in') and a lack of the necessary skills or knowledge. The lack of skills or knowledge may not just be in the designing and deployment of Wireless LANs but also in the complex computer based services necessary for a secure and scalable Wireless LAN, such as RADIUS.

For enterprise customers, these new technologies not only offer potential improvements on revenue, profitability and cost management, but also offer the potential of consuming large amounts of unplanned time and budget. Getting it right from the start is essential. Getting it wrong can absorb too much time and unnecessary expense.

This paper describes an approach that will assist enterprise organizations in 'getting it right' first time. It shows how the various needs, desires and applications can be delivered. It does not discuss the specific implementation of any products or technology (see other Madge materials and papers for additional information on products and technologies).

2 The business benefits of Wireless LANs

A Wireless LAN provides the same 'mechanical function' to a wired LAN. Simply, it connects users to their networked resources, usually providing the final link between the user's PC or workstation and the network concentration point. However, it makes this connection in a way that offers mobility and flexibility that is impossible with wired LAN connections. This enhanced mobility and user location flexibility is the key to increased productivity and reduced costs. Wireless LANs can be used outside of the users' usual working areas - the security implications being a cause for concern, outside of the building - a greater cause for concern and even whilst travelling through the use of public Wireless 'Hot Spots' - an even higher cause of concern.

In addition, this new mobility also enables exciting opportunities by enabling new applications (warehousing and paperless workflow processing being examples). The user's working environment is extended beyond the traditional reach of physical LAN cables, and new applications can be exploited. This application integration is further enabled with handheld devices (PDAs, palmtop and Tablet PCs and other devices which have a single specific data management purpose).

To be most competitive, enterprises must remain flexible and responsive to the dynamism in their own market sectors. However, this becomes more difficult the bigger the enterprise becomes. Many users in enterprise organizations move and change role, desk positions, buildings and even locality

on a regular basis (this is often referred to as 'churn'), and a user in an enterprise might churn annually 2, 3 or perhaps 4 times. Managing a physical infrastructure is time consuming and, with the trend towards smaller IT management resources and ever-tighter cost control, the overhead of managing the existing topology can inadvertently become an obstacle to business flexibility. Although Wireless is sometimes perceived as being yet another technical challenge, Wireless delivers real productivity gains and cost saving for the IT department. It changes the network's physical architecture into a logical architecture. As a result, Churn is easier to manage because changes that traditionally required physical re-patching and manual interventions can now be accomplished at a management screen – if required at all. However, for a successful deployment the workload, skill-straining and other resources necessary for the deployment of Wireless technology must be minimized.

Wireless LANs obviously require fewer cables and physical user concentration ports, so equipment capital costs are reduced.

In fact, any enterprise currently considering the deployment of new or additional Ethernet workgroups should consider bypassing Ethernet technology and quickly adopting Wireless where possible. Today's common 11Mbps Wireless LAN products (802.11b) may not be able to provide wholesale LAN replacement for all applications in all organizations, but it is complementary. Newer Wireless LAN technologies (e.g. 802.11a and 802.11g) offer higher speed and throughput, and can be considered a replacement for wired LANs.

3 The 'Wireless Imperative' and its challenges

Clear business advantage results in a real sense of urgency and this applies to Wireless LANs. Wireless LANs, if correctly deployed, offer increased competitive advantage, greater business flexibility and lower costs. This is the 'Wireless Imperative'.

However, as stated earlier, enterprise organizations face a number of barriers to the successful implementation of secure and scalable Wireless LANs. From Madge's customer research activities in the enterprise sector, we have determined the primary barrier to be security.

3.1 The Security Challenge

Security is of tremendous concern for enterprise organizations. The Madge Q1-2003 customer research indicates that 60% of enterprise customers identify security concerns as being the primary barrier to their adoption of Wireless LANs. These perceived problems are exacerbated when equipment from multiple vendors are used as each vendor may implement security management in their own (perhaps proprietary) way.

Of course, radio transmissions of data travelling between the user's PC and the Wireless concentration point ('Access Point' or 'AP') must be protected against eavesdropping and intrusion (e.g. 'man in the middle' attacks). However, the real nightmare scenario for IT Departments is the attack on the wired enterprise data and services coming from a less controlled Wireless client (a sense of well being, safety and 'being in control' is often derived from physical LAN cables). If an organization has invested many hundreds of millions of dollars into their core business applications, services and data, the last thing it needs is unauthorized access by Joe Public who is conveniently situated outside the building. Hacking may be malicious, or simply a way for Joe to access high bandwidth, free Internet connectivity. Either way, appropriate security is essential.

Authentication is one vital element of security, but so is encryption of transmissions. Traditional WEP implementations ("Wired Equivalence Privacy", a way of securing data transmissions through the use of encryption keys) using 'Static WEP keys' may be OK for a SoHo customer but are, in no way, acceptable for enterprise customers where (for example) the theft of one laptop can easily open up the network to very damaging intrusion. Static WEP keys can also be learned relatively easily using

tools available, free of charge, from the Internet. Static WEP keys need to be changed very regularly, and it is the overhead of Static Key management (or lack of) that leaves many organizations vulnerable to attack. In practice, because of the management time and overhead required, Static WEP keys usually remain unchanged rendering them useless.

A detailed consideration of these security issues can be found in the Madge Wireless LAN Security White Paper (WWP-001).

3.2 The Integration Challenge

Integration quickly becomes a challenge. With multiple Wireless vendors, multiple Wireless technologies, varied and very complex (but existing) networks (including Gigabit, 10/100 Ethernet and 4/16/100 Token Ring) and applications, coupled with ever reducing IT support resources, successful integration becomes a key strategy in meeting the challenges faced by IT departments.

However, Wireless integration involves much more than connecting a Wireless LAN to a wired LAN. To plan and manage effective Wireless LAN deployment within an enterprise organization requires a great deal more than simply purchasing some Access Points (APs) and Wireless Network Interface Cards (NICs), as one might do in a SoHo (Small Office / Home Office) or SMB (Small and Medium Business) environment. For example, a secure and scalable enterprise Wireless LAN requires *authentication services* (itself requiring the integration of multiple technologies to support user identification and authorization), *dynamic encryption services*, *firewalls*, *VPNs*, *DHCP services* and *infrastructure and policy management*. The separate deployment of these functions is challenging. Each function is complex in itself, and pulling them all together so that they work together seamlessly can take weeks. In addition, the ongoing management of separate functions (in endeavouring to perform a single management task, such as simply adding a user) is difficult, impractical and costly.

Small problems encountered during a Wireless LAN pilot installation could be exponentially multiplied as the network grows in size and as equipment from more vendors is added over time.

3.3 The Multi-Vendor Management Challenge

There are two key challenges to Wireless management: the management of the Wireless devices themselves, and the administration of the security services (e.g. 802.1x authentication and Dynamic WEP) of these devices. However, with the Multi-Vendor, heterogeneous, nature of today's IT infrastructures, how does an enterprise organization manage authentication, dynamic encryption and AP device management when the APs may come from a variety of vendors whose own management platforms will only manage their own devices? A number of vendors do provide "Multi-Vendor management", but this is usually only for either device management or Security administration.

If overly complex management scenarios are to be avoided, then the network management application must manage both devices and their security services. The ideal solution is a Vendor Independent solution.

3.4 The Skill and Expertise Challenge

New skills are required when installing the necessary supporting software services, often purchased from different vendors (including Certificate Authorities, client Authentication servers and dynamic encryption) and configuring them to work together in a coherent manner is challenging, time consuming and expensive. This is without the added challenges of coping with using device management platforms from multiple vendors.

3.5 The Future Proofing Challenge

Although many Wireless devices are already in a 'commodity sales' phase, the Wireless industry, its standards and underlying technologies are still relatively young and are rapidly developing. The enterprise customer has a seemingly impossible challenge of implementing a network management platform that will change and grow in a way as yet unforeseen, and yet will integrate unforeseen developments in technology and products. 'Single technology', single vendors or proprietary solutions should be avoided, unless a customer makes a specific decision to adopt a proprietary solution for a specific purpose. Vendor specific packages are good for device management and security management for that Vendor, but the market is simply too dynamic for this to be a solid strategic step at this time.

Also to be avoided is the short-term attractiveness of purchasing an array of 'low cost' SoHo or SMB Wireless LAN products. Products targeted at SoHo and SMB customers have specific features and functions for these markets, but are not always appropriate for enterprise deployments - especially when the Wireless LAN grows to 100, 1,000 or even 10,000 users. One can imagine the overhead and potential pitfalls of scaling a Wireless network, originally designed for 10 users, up to 1,000 users.

The key characteristic of the Wireless market is change, which can result in confusion and uncertainty for customers. Future proofing, as far as it possible, must feature on the list of essential ingredients for the enterprise.

4 Meeting the 'Wireless Imperative'

Implementing and supporting a secure and scalable Wireless LAN is challenging (and rewarding for many). Yet, the 'Wireless imperative' exists. Enterprise organizations must quickly seize the opportunity for lower costs, improved efficiency and increase competitive advantage. Where possible, new user deployments or additions to existing Ethernet networks should be considered as prime candidates for Wireless. It is a fact that Wireless is an everyday LAN technology.

In summary, the key challenges for enterprise organizations in planning Wireless LANs are:

- Security.
- Integration and Management.
- Multi vendor AP security and AP device management, and interoperability.
- Future proofing and flexibility.
- Wireless design, deployment and support skills.
- Taking early advantage of Wireless.

5 Requirements for Enterprise Wireless LANs

This section details the key elements necessary for the successful, structured deployment of an enterprise Wireless LAN. It does not endeavour to discuss detailed planning, but discusses the items that need to be planned, in advance of any Purchase Order for equipment and software.

5.1 Standards Compliance

It is important for enterprise customers to adopt a standards compliant approach, and must be very wary of both (sometimes hidden) proprietary technologies and pre-standard 'lock in'. An example is EAP (Extensible Authentication Protocol), which is a standard 'container' for carrying authentication

information. However, the authentication protocol itself, used by a vendor to perform authentication, within EAP might be proprietary. So, although a vendor may claim EAP compliance, their solution might be proprietary.

In addition, the Wireless market is changing, so, a secondary consideration to standards compliance is the ability to enhance the platform at a later date to accommodate new technologies and standards.

5.2 Device and Security Management

The ongoing (and ultimately more significant) cost of any network is in management and running costs. There are two key aspects of Wireless LAN management - device management and security administration. Some Wireless management applications provide limited 3rd party device management or 3rd party security management, support for 'other vendors' equipment is limited.

It is highly recommended that, to avoid the necessity to install and maintain multiple management platforms, and to avoid unplanned future management software migrations, the customer should implement a modular, multi-vendor security and device management application from day one. The key requirements for the Wireless management platform are:

- Device management of multi-vendor Access Points using SNMP.
- Security administration of multi-vendor Access Points.
- Modularity to support new products, technologies and standards as the Wireless industry and technologies develop and change.
- Scalability from 5 users to 1,000s of users.
- Compliance to industry standards.

5.3 Device and User Administration

A large-scale enterprise Wireless network requires a number of software services. Each software service requires, in most cases, a separate hardware platform and these services must then be configured to communicate with each other in a coherent way. During the planning of the network, the enterprise customer will consider all of these costs in terms of hardware, software and services integration. In reality, it is this degree of cost and complexity that can dissuade some enterprise companies from piloting Wireless, despite the potential business benefits.

These additional services includes the provision of authentication information (e.g. a Certificate Authority or 'CA'), a method for performing the client authentication (e.g. a RADIUS server), firewall to protect the wired enterprise LAN from Wireless intrusion, a service for secure, remote Wireless management platform access (e.g. VPN), Wireless traffic security (e.g. dynamic WEP encryption administration) and SNMP enabled management services for the Wireless devices.

After a very short planning exercise, it will be clear that a highly integrated solution is the quickest and easiest to deploy, thus presents the lowest installation complexity and ownership cost.

5.4 Vendor Selection

Ensure that the potential Wireless vendor has a pedigree and demonstrable expertise in enterprise, multinational networking appropriate to the size of the challenge. A SoHo or SBM solution is probably technically and commercially the wrong solution for enterprise organizations.

5.5 Implementing a Successful Architecture

The term architecture is important. It is proposed that enterprise organizations use 'models' to define their architecture. It is also proposed that the enterprise organization should design their Wireless network to be 1000 nodes in size on day one. Of course, it is highly unlikely that any enterprise organization will deploy a 1000 client Wireless network overnight. They will probably test and pilot a chosen solution and then more widely deploy the technology and applications. However, by modelling the network in this way, the customer can be more assured that the new Wireless LAN will accommodate this user count.

In other words, you will have built scalability (of both management and security services) into the network. Put simply, if one endeavours to scale a Wireless LAN designed for 50 clients to 1000 clients, there are likely to be significant problems as the network grows in size. However, modelling the right architecture will save time and money later on, and (assuming that the chosen solution provides modularity and scalability) the immediate costs will probably be the same.

5.6 High Level of Integration

A small scale, or pilot, Wireless LAN may seem to represent a high '\$ per user' cost when the user count is small, because the organizations may need to implement Certificates, RADIUS services, additional firewalls, VPN, DHCP and other services. A highly integrated solution is the key to:

- Managing the early deployment costs and workload.
- Scaling the network to enterprise size.
- Managing ongoing costs.

5.7 High Level of Modularity

To accommodate the rapidly changing characteristics of the Wireless LAN market, a modular management platform will allow an enterprise customer to react rapidly to change. This modular platform is better able to accommodate:

- The management of Wireless LAN equipment from multiple vendors.
- The security administration for multi vendor equipment.
- New services, standards, technologies of products.
- Rapid expansion and change.
- Scalability accommodating unforeseen growth.

Ensure that the management application offers both security management and multi-vendor device management in a single application. It must also scale from 5 to 1,000 clients without having to change the application, and it must be equally cost effective in 5 and 1,000 client configurations.

Network management environments can be very complex, especially where multiple services are expected to cooperate. This complex array of functions can lead to errors or omissions in coordinating changes across different platforms, potentially leaving security holes in the network. If possible, implement a management application that is easy to use and one that masks the complexity from the administrator. For example, client or device configurations requiring coordinated adjustment to settings in more than one service can lead to a multi-step user management processes. A scalable Wireless solution should integrate this complexity in a series of single operations or settings, where the complexity of making adjustments to a number of functions is, as far as is possible, masked from the network administrator. For example, adding new users or devices should be fast, simple and safe.

Madge recommends selecting a management application where the various actions required of the user (authentication, network logon, Windows logon and encryption key setting) are integrated into an easy to use dialog that masks the complexity to the user, making the experience pleasant (ideally unnoticeable).

5.8 Appropriate Security

Implement only the security services necessary to deliver the security you need. For example, implement 802.1x for enterprise Wireless LAN security, and use VPNs for those communication paths that require virtualisation (i.e. enterprise access through public 'Hot Spots'). VPN is not necessary for everyday Wireless LAN clients, but may be required for the remote management of Wireless domains over the Internet. Again, this calls for modularity, where different services can be added to the Wireless architecture as the network develops. Enterprise customers should avoid the pain of making their security arrangements too complex and inappropriate to the need. Madge Customers are advised to adopt 'models' help in the design and implementation of appropriate security services. Madge proposes their 5-Element Security Model, full details of which can be found in the Madge Wireless LAN Security White Paper (WWP-001).

Madge's key recommendations for Wireless LAN security are:

- Deploy an extensible, standards-based security architecture.
- Implement 802.1x EAP-TLS with per-session WEP keys.
- Implement mutual authentication using digital certificates.
- Use centralized policy based security.



VPN



Firewall



Authentication



Encryption



Device Authorization

6 Key Recommendations

In summary, the key recommendations for a Secure, Scalable Enterprise Wireless LAN architecture are:

- Design an enterprise architecture that has inbuilt scalability, using models for simplicity.
- Implement a highly integrated management design, minimizing the number of separate platforms and service applications.
- Employ a modular management application to accommodate the fast changing market.
- Ensure the accommodation of both SNMP device management and security administration for Wireless equipment from multiple vendors.
- Use appropriate security services.
- Use Wireless for all new user deployments and significant workgroup changes, where possible.