



White Paper

## Justifying the Wireless Enterprise

# Executive Summary

- ✂ This white paper explores a broad range of Wireless LAN business and financial benefits.
- ✂ Wireless LANs provide increased mobility, save time, increase staff productivity, and dramatically reduce the costs of office moves, within a secure authenticated network.
- ✂ The Wireless LAN Products boost your business with a lower Total Cost of Ownership (TCO) and higher Return On Investment (ROI) than that for traditional wired local area networks.

## 1 Introduction

### 1.1 Why Wireless?

Wireless technology has brought about great benefits in terms of employee productivity through mobility. Its ability to provide location independent access to real time information empowers workers to make quicker better informed decisions. Also the ability of an organisation to have instantaneous visibility of its' assets, be they goods in transit or a parcel delivery truck, are all thanks to wireless. This is coupled with the proven figures that the capital cost of deployment for a Wireless LAN user is much lower than that of the provisioning of a user connected to the wired LAN.

### 1.2 Market Acceptance and Sizing

During the last 3 years local area Wireless networking has started to become a mainstream enterprise networking technology on a worldwide basis. The overall WLAN marketplace is expected to be worth more than more than \$6Billion by 2006, of which the enterprise marketplace (infrastructure and clients or wireless adapters) is just under 50% of the total value.

### 1.3 Justifying the Investment

Many customers ask us to try and quantify the benefits of Wireless networking. These can generally be summarised as either being qualitative business benefits, or quantitative financial benefits. In common with new networking technologies such as the arrival of the Internet in the mid-1990s, the Total Cost of Ownership needs to be seen as just one aspect of the business decision.

Madge believes that during the next 5 years, most enterprises will boost their business and staff mobility through the deployment of Wireless network extensions, in the same way that during the last 5 years, practically all enterprises have deployed Internet & intranet extensions.

## 2 Business Benefits

### 2.1 Mobility

Wireless provides the "invisible infrastructure" that allows staff to work wherever they need. Mobility is particularly useful, with a proven ROI for many applications, in large manufacturing facilities, warehouses, chemical plants, transportation depots, airports, hospitals, hotels and convention centres. As security concerns have now been allayed the 'next wave' of wireless will be the deployment in enterprise offices.

The advent of the laptop computer has already moved us towards this new world of flexibility and freedom. The majority of computer vendors are already incorporating 802.11 wireless capabilities in

all but entry level laptops, indeed Gartner predicts that '85% of laptops and 60% of handhelds (are) expected to be wireless enabled by 2006'.

## **2.2 The Portable Office**

The "portable office" is now defined as the place where YOU want to transact your business.

Many Business executives already benefit from the advantages of Wireless networking that is available in Wireless "Hotspots" that are now being deployed during in major hotel chains, conference centres, coffee shops and airline lounges. At the end of 2004 this represented in excess of 46,000 locations worldwide, with the numbers forecast to grow exponentially; InStat/MDR predict that there will be 200,000 hotpots by 2008. This provides staff with greater flexibility in accessing their email and the Internet, planning their meetings, and networking with their teams, customers and partners.

## **2.3 Saves Time: Faster Decisions and Services**

Working with Wireless means continuous connections with your enterprise network as you roam the office, conference room and company rest areas. In addition, a secure Virtual Private Network (VPN) tunnel can be established to enterprise servers running over public Wireless "hotspot" networks and the Internet. This allows busy executives or 'road warriors' to access sensitive corporate data, in a completely secure way, whilst away from the office on important business trips.

Other applications could include field engineers and support staff that may need to access critical information whilst working on their client premises or other sites providing Wireless access.

## **2.4 Improves Productivity**

In a survey performed by NOP World- Technology, it found that users remained connected to the network, on average, for an additional 1.75 hours per day. This translated into 70 minutes of additional productive work per day, which in turn meant increased productivity of 22%. When taken across a medium or large enterprise, this could have quite dramatic impacts on the "bottom-line" (potentially \$Ms), and release more cash for investment in future strategic projects and ventures.

## 3 Financial Benefits

### 3.1 Criteria to be considered

Calculations of Financial Business Indices such as Total Cost of Ownership (TCO) and Return on Investment (ROI) are very much dependant on definitions, and the specific business environment in which the Wireless network is established and operated. In this white paper we'll make basic assumptions in order to compare the options of extending an existing Ethernet or Token-Ring network using a Wireless network rather than expanding the existing wired network.

The key TCO criteria are:

- ✂✂ LAN Cabling Costs: Installation Labour Costs and Cables.
- ✂✂ Costs of 10/100 Ethernet Hubs and/or Switches.
- ✂✂ WLAN Infrastructure: Access Points, Cables, and Power over LAN.
- ✂✂ Network Management and Security Costs: Both Wired and Wireless.
- ✂✂ Infrastructure Costs of office moves and changes.
- ✂✂ Wired or Wireless Client Adapter Cards: Component & Set-Up Costs.

### 3.2 TCO: Wired vs. Wireless Networks

Based on the above criteria, we'll make a straightforward comparison of the TCO for Wireless networks compared with wired network extensions for 500 enterprise users on a single site.

#### 3.2.1 Fixed Costs

- ✂✂ Madge Wireless LAN Equipment (and Ethernet "back-haul"):
  - ✂✂ 500 Internal Client Adapters (NICs) @ \$40 = \$20k
  - ✂✂ 40 Access Points @ \$400 = \$16k (Enterprise Grade including SNMP/Security)
  - ✂✂ 40 Ethernet switch ports = \$3.2 (Assumes \$80/port)
  - ✂✂ 500 Device Enterprise Access Server Software Licenses @ \$80 = \$40k

TOTAL Cost of Wireless LAN Equipment = \$79.2k

- ✂✂ Wireless Network Installation:

- ✂✂ Wireless NICs = \$12.5k (15mins/NIC @ \$100/hour IT Staff Cost)
- ✂✂ Wireless APs = \$4k (60 minutes/AP @\$100/hour IT Staff Cost)
- ✂✂ EAS = \$4k (Based on 5 Days @ \$800/Day IT Staff Cost)
- ✂✂ Cabling to 40 Access Points @ \$100/Drop = \$4k

TOTAL Cost of Wireless Installation = \$24.5k

**WIRELESS Fixed Costs: TOTAL cost of Wireless equipment & deployment is: \$103.7k**

- ✂✂ Wired Ethernet LAN Network Extension (Equipment and Installation – 10/100Mbps):
  - ✂✂ Ethernet Switches and Clients = \$40k (Assumes \$80/client)
  - ✂✂ Cat5 Cabling and Installation Costs – 500 Clients = \$50k (\$100/client)
  - ✂✂ Network Management & Security = \$28k (Assume \$40/Client and 10days set-up cost)

**WIRED Fixed COSTS: TOTAL initial Cost of Wired Network Extension = \$118k**

### 3.2.2 Variable Costs

- ✂✂ Wired users: Costs of Network Moves and Changes:
    - ✂✂ Assume 25% of users move office twice each year – i.e. 50% changes/year
    - ✂✂ Assume Basic Cost of moving each user is ~\$100/user (wired users only)
    - ✂✂ Also assume ~\$5k Network Management/Server Re-configuration (each major move)
- Hence annual costs of moves =  $(500 * 0.5 * \$100) = \$25k$   
 And Network Re-Configuration (two major moves) = \$10k

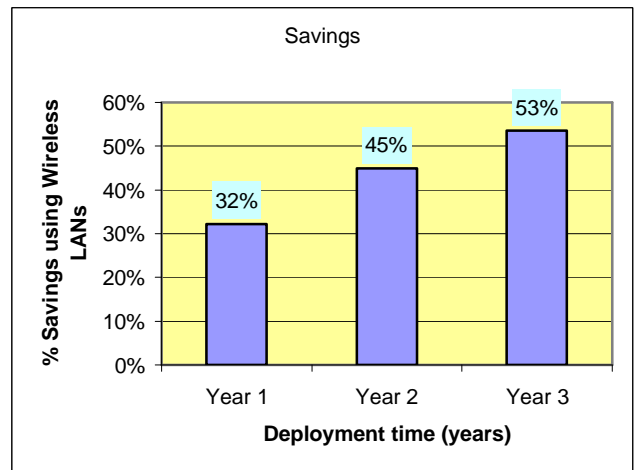
**WIRED Variable Costs: TOTAL costs for Wired Network Moves/Changes = \$35k/year**

- ✂✂ Wireless users: assume these are fully mobile so moving costs are \$0k (zero).

**WIRELESS Variable Costs: TOTAL costs for Wireless Network Moves/Changes = \$0k/year**

In summary, this quick analysis would suggest that Wireless Networks for ~500 users could cost around 32% less than Wired Ethernet deployment during the course of the initial 12 month period (Wireless - \$103.7k vs. Wired - \$153k). The equivalent savings after 2 years and 3 years wireless deployment increase respectively to 45% and 53% due to the relatively high cost of making moves/changes and network reconfigurations within wired networks.

In addition, the expected price decreases in WLAN components for wireless infrastructure and clients will make the TCO savings even more compelling for CIOs & IT Management.



## 3.3 Practical Ways Forward for your Enterprise

As stated, the above analysis is highly dependent upon the specific details of your deployment environment, regional IT labour costs, as well as the office dynamics with regards to staff moves and changes. It is suggested that you rework the above analysis with your own data to fully understand the economic benefits of Wireless deployment over a suggested 3-year period.

## 3.4 Wireless Return on Investment (ROI)

The greatest business impacts for Wireless LANS are the productivity benefits for staff working at *all* levels of the organisation. For instance Intel Finance (Intel Corporation) undertook a major survey of such Wireless LAN productivity savings amongst engineering, manufacturing, sales, marketing and

support staff. The resulting ROI analysis (Net Present Value - NPV) based upon various sized buildings over 3 years are compelling:

- ✂ Small Building (32 users): Net ROI: \$280k
- ✂ Medium Building (150 users): Net ROI: \$940k
- ✂ Large Building (800 users): Net ROI: \$4,600k

For further information on the Intel Corporation study we suggest that you access the full report, which is available from the Intel web site ([www.intel.com](http://www.intel.com) and search for 'Wireless LAN ROI').

It should be understood that these impressive ROI figures include the full cost of the Wireless equipment, installation and configuration costs, as well as operations, depreciation, taxes and the productivity savings broken out according to the size of each category within the workforce.

## 4 Further Wireless LAN Topics

Despite the compelling TCO and ROI financial benefits, there are still those that resist Wireless deployments due to other issues that emerged during the experiences of the early adopters of the mid to late 1990's. These situations have been further compounded by the amount of negative publicity centred on hackers gaining access to enterprises networks through unofficial or 'rogue' wireless infrastructure. However, robust solutions are now available for *all* enterprise users to these issues that concerned early users, to quote a well respected analysis organisation, Infonetics:

*'It's really a case that enterprises may need some help understanding how to secure them, but the technology is there.'*

### 4.1 Network Security

Madge Wireless products meet all the requirements of enterprise-grade security, as well as the US Health Care Privacy and Security needs (HIPAA). In particular, the Enterprise Access Server, Access Points and Client Adapter Software all support the most rigorous security that includes:

- ✂ Mutual Authentication of Client and Server using IEEE 802.1x.
- ✂ Integral RADIUS and Certificate Authority within the Enterprise Access Server.
- ✂ Dynamic selection of encryption keys for each session.
- ✂ Dynamic rotation of encryption keys during the user session (e.g. every "x minutes").
- ✂ Integral Firewall and VPN Security Software within the Enterprise Access Server.

In all, Madge provides a robust 5-element security model that allows enterprises to choose which level of security they wish to implement and tailor for their specific business operations. The security hazards and wireless "hacker threats" from the 1990s are now closed and solved for enterprise wireless networks based on the Madge product family.

### 4.2 Wireless Intrusion Detection Systems (IDS)

A major challenge for I.T. managers is the rapid growth of readily available and easy-to-use wireless networking equipment. Without an effective policy plus control and management, this equipment will compromise network security. A wireless-enabled enterprise will have hundreds of Access Points and many wireless users. Unauthorized Access Points can potentially be installed at any wired Ethernet port, which is a major security threat.

Even if an enterprise has mandated a no-wireless policy, with the proliferation of wirelessly enabled devices and the low cost of SOHO style wireless infrastructure, the threat of a wireless 'backdoor' into the wired network still remains.

In order to enforce a controlled wireless access policy or impose a 'zero wireless' approach, a comprehensive method to managing the wireless infrastructure should include:

- ?? Setting and the enforcement of wireless LAN (WLAN) and Bluetooth policies
- ?? Monitoring authorized and rogue access points
- ?? Detecting intrusions and attempted attacks
- ?? Identifying unapproved networks and connections
- ?? Identifying incorrect configurations that can lead to new threats
- ?? Understanding and managing wireless network performance
- ?? Disruption of unauthorized conversations with the trusted wireless network

An enterprise may believe they have a controlled wireless network or an effective no-wireless policy, but *only* a comprehensive wireless IDS (such as the Madge WLAN Probe Monitor 2) will let you know what is really happening in your airspace. It answers questions like "who's talking to who – do I trust them?", or "how many Access Points are there on my network, and are they all authorised?"

Madge is at the forefront of IDS development and, indeed, have moved IDS on into its 3<sup>rd</sup> generation where **detection** becomes **Proactive Protection**.

## 4.3 Single or Multi-Band Wireless LANs

Until recently the selection of IEEE 802.11b has been the rational choice for enterprises in their deployment of wireless LANs. During 2004, however, many enterprise vendors (including Madge) have introduced wireless infrastructure capable of supporting the higher speed (54 Mbits/Sec) IEEE 802.11g. This is now the de-facto standard for new enterprise roll outs and has the added advantage of being backwards compatible with the well established 802.11b infrastructure and clients.

As the 2.4Ghz band (that 802.11b and 802.11g both operate in) becomes much more utilised then increasingly enterprises will need to look (in 2005 and beyond) to 802.11a for applications that demand high bandwidth or are particularly sensitive to delay, such as Voice or Video.

In summary:

- ~~✂~~ 802.11b: 11Mbits/Sec: 3 Simultaneous Channels available – worldwide.
- ~~✂~~ 802.11g: 54Mbits/Sec: 3 Simultaneous Channels available – worldwide.
- ~~✂~~ 802.11a: 54Mbits/Sec: 8 Simultaneous Channels available - some restrictions.

The Madge strategy is to:

- ~~✂~~ Design and engineer ALL Madge wireless products to industry standards.
- ~~✂~~ Ensure that the Enterprise Access Server is developed according to modular architecture.
- ~~✂~~ Develop loadable software modules to support a range of enterprise Wireless Access Points.

Madge is shipping the Enterprise Access Server (EAS), which has support for 802.11g and is 802.11a "ready", in addition to supporting a range of legacy enterprise 802.11b Access Points. In

this way, users that choose to implement the EAS Management and Security software today can be sure that their solution minimises the risk of premature obsolescence due to dynamic standards.

Madge, in common with most other leading enterprise WLAN vendors, expects customers to move from single-band/single-radio, to multi-band/multi-radio Access Points and Adapter Cards during the coming 12 to 18 months. The fact that EAS has “in-built” options to support loadable SNMP Management modules for the complete spectrum of 802.11 standards makes this a sure bet decision for CIO's and IT Management that wish to minimise both costs and risks.

## 4.4 Wireless Industry Standards

The final issue that we've already touched upon above is that of Wireless industry standards. In addition to the 802.11 transmission/protocol standards there are various evolving standards for wireless security, as well as inter access point Wireless roaming, Quality of Service (QoS), and power over Ethernet (POE).

A key reason for choosing Madge is that we have strict policy and strategy only to implement and launch products once the relevant standards have been defined and ratified. In the past, some vendors have deployed proprietary standards that effectively lock you, as customers, into a closed architecture with all the corresponding implications regarding prices & integration.

Choosing Madge, means that you buy into an “open world” of integration through industry standards such as Multi-Vendor, SNMP Management, IEEE 802.1x mutual authentication based upon robust EAP-TLS certificates and enterprise-grade scalability through LINUX software that operates on any approved INTEL based Server.

## 5 Summary

In summary, Madge reduces your total cost of ownership through an architecture based on industry standards that integrates all the key components (including 5 element security model, scalability and multi-vendor SNMP management) within the Enterprise Access Server.

The Enterprise Access Server (from 5 to 1000's of users) is robustly engineered to be your secure enterprise gateway or switch between your “Wireless world” and “wired world”.

Once the wireless LAN has been installed and is being managed then the final stage is to protect it, using Madge Probes and the Probe Monitor 2. Working in concert they provide an effective Wireless Intrusion Detection System that detects and logs rogue wireless infrastructure and clients. identifies unauthorized wireless conversations for 802.11a/b/g (and Bluetooth) and uses 'Countermeasures' to disrupt rogue clients.

The breadth of features and functionality on these pioneering products is unique within the world marketplace today.