

## **Planning for WLAN – Enterprise Class**

By Calum Lamont, Director, FarrPoint

### **Introduction**

This paper looks at the issues to consider when deploying enterprise class Wireless LAN within your organisation. At the outset, the definition of enterprise class is to differentiate between the low cost home based WLAN products which do not scale or have the ability to integrate into the corporate network in a secure and manageable manner. Enterprise class WLANs are designed to be scalable, to provide leading security controls and to be integrated and fully managed with the corporate network.

WLAN technology has developed greatly over the last few years to provide a well regarded functional platform for increasing flexibility of the workforce. Differences in architecture, security and management features are the most obvious choice between vendors. However, there are other differences which need to be considered and a number of questions to answer before deployment.

The benefits WLAN can offer organisations in terms of increasing flexibility are quite clear. WLAN enables flexible and mobile working and allows the corporate network to extend beyond the traditional work areas. This can provide efficiencies in working practice and allow continual access within and around buildings for both voice and data and associated applications.

For some markets WLAN can also be coupled with applications like location tracking which allows automation and interfacing with back end systems for many tasks such as stock taking, asset tracking, location tracking, and theft prevention.

## **WLAN Strategy**

Many organisations decide to deploy WLAN to offer an alternative option to their wired desktop connection, with this being their main motivation. Whilst this can indeed be a good reason in itself, the deployment of wireless can open up many more options for provision of services with new applications and ways of working which can be supported. As an initial step, we recommend that a strategy for WLAN should be developed which will identify the benefits to the business of deploying the technology. This should not be done in isolation but should look at all the communication needs of the organisation to capture the range of requirements and understand how wireless can provide support. Users in many organisations expect wireless access and organisations can lose revenues from not providing it in a well thought through manner.

There are a number of questions to answer when developing the strategy. How might business processes be affected by the ability of wireless? Will the flexibility of location mean that tasks can be completed differently or more efficiently? For example, how might this support home working by implementing secure Wireless Access Points which extend the security boundary of the corporate network in to the user's home? What additional features can be deployed now that assets can be tagged and presence monitored? Will voice and video applications be required? With Quality of Service and the release of higher capacity 802.11n technology, applications such as video become a more realistic option. The technology is now capable; it is the way organisations uses the capabilities which need to be thought through.

WLAN can also be used to provide coverage in outside areas such as student areas, recreational areas, work areas and more specialised areas such as loading bays. The potential use of wireless in all these areas should be considered. In addition, low cost

building to building connections can also be provided and any such requirements should be built into the overall requirements to be met by the wireless deployment. There can be benefits in providing this functionality through the same vendor in order to manage the complete wireless systems under a single management platform.

## **Design**

There are a number of elements which make up the design of the system and vendors can provide elements of the design services, if necessary. It is important, however, for the organisation to understand these issues so that they know what to expect, be aware of the process involved and maintain control of the overall strategy.

Most Enterprise WLAN solutions are made up of Wireless Access Points (WAPs), Wireless LAN Controllers and Management software. The topology of Controller deployment needs to consider the existing LAN and WAN network infrastructure, resilience requirements, user numbers and budget. Different topologies of central controllers, distributed controllers, a mix of both or even solutions with no controllers but more intelligence in the WAPs, all make a difference to the final solution.

Management software is fairly well established with common functionality between vendors but subtle difference in usability mean they really have to be demonstrated and preferably trialled to test suitability. Good management will be key to providing a consistently excellent user experience while ensuring security of both the wired and wireless networks.

WAPs are of course the most crucial element as they provide the access to the network and so determine the coverage, capacity and overall performance.

The decision on the level of coverage to be provided will define the services that can be supported and the investment required. Coverage is often identified as an area where a wireless connection can be obtained. But the lower the signal received from the Access Point, the lower the speed of connection. So it is important to consider what speed is required to successfully support the applications you wish to deploy over wireless. This includes agreeing the speeds required at the edge of the coverage cell where speeds will be lowest.

In addition if your applications require seamless roaming between Access Points as users move around the building, important for many handheld devices and especially for IP telephony over the WLAN, coverage holes at the cell edge must be avoided.

Along with coverage, capacity must also be considered and additional infrastructure may be required for busy locations so that speeds available to users are maintained. WAPs are limited in the number of users they can practically connect (regardless of vendor's claims!) and dependant on what these users are doing, this will impact on the overall user experience. Areas where there are high densities of users such as classrooms, lecture theatres, open plan offices, may need additional capacity as well as good coverage. In this case, several co-located WAPS may be required which often requires careful radio planning to avoid radio interference problems. As a result, it is easier to assess this likely demand at the outset and get the design done right from the start.

The latest WLAN standard is 802.11n which provides greater capacity and coverage and operates over the two main frequency bands used by WLAN. Most clients currently do not

support 802.11n as standard and instead support the older and much more common 802.11a/b/g standards.

The design should therefore consider how these clients will be supported and how the benefits of 802.11n will still be made available despite this backward compatibility requirement. Some important considerations here are the power requirements for simultaneous use at both frequency bands and all protocols, and the LAN capability to adequately support the bandwidth capabilities of 802.11n. To get the benefit of the additional speed of 802.11n will require Gigabit Ethernet wired ports which may require a LAN refresh.

A final consideration with WAPs is the aesthetics. Some of these units can look downright ugly (one vendor's product is nicknamed the 'face grabber!') and sprout multiple antennas whilst others are much more unobtrusive and may blend into the building environment much more successfully.

## **Security**

Security is always a concern with WLAN, however with the strong encryption and authentication services available today these issues have been addressed. However, as with any networking technologies there are still threats and vulnerabilities that need to be considered. Some of these issues are:

- How will users authenticate with the organisation's systems?
- On successful authentication, what resources will the user gain access to? Will these be the same as on the wired network, or a subset of these?

- Is authentication always required? For example, this is not normally needed for guest access but control will likely be required on what they can access e.g. Internet only, and how long their access is valid for.
- How will the organisation manage the content available to the Guest? For example, there may be a policy on which web sites can be accessed and filtering may be required.
- How much can a mobile user's device be trusted and will Network Access Control (NAC) be required to remediate, quarantine and upgrade user devices to ensure that devices connecting to the wireless network have an up-to-date Anti-Virus and Operating System. This is especially important for mobile devices.
- Preventing 'Rogue' wireless devices joining the network is important to avoid people connecting their own wireless devices in to the network. This can be malicious or even fairly innocent users attempting to set up their own wireless access.

## **Conclusion**

This paper has outlined some of the considerations which should be taken in the planning of WLAN deployments. Investing in the planning stage and developing a thorough strategy for how wireless can help your business processes, can reap benefits and ensure a successful deployment.

A poorly thought out and unreliable wireless network will quickly become a burden as users now demand a consistently reliable wireless system that offers the same experience as the wired infrastructure.



Wireless can do more than offer an alternative way of connecting your laptop to the network and with some thought can be the catalyst for smarter ways of working and increased efficiency across the workplace.

**About FarrPoint**

FarrPoint are leading independent consultants offering impartial technology advice to improve our client's business. FarrPoint specialise in networking, IP telephony and convergence technologies and provides services of strategy and design, specification and sourcing, project management and network efficiency and technology reviews.

Contact W: [www.farrpoint.com](http://www.farrpoint.com) E: [contact@farrpoint.com](mailto:contact@farrpoint.com) T: 0131 202 6018