

Best Practices for Deploying Wireless LANs

An overview of special considerations in WLAN implementations

As wireless LANs (WLANs) continue to grow in popularity, particularly in enterprise networks, the ability to do away with massive amounts of cabling to the desktop is one very obvious advantage. There are many more. Mobile, ubiquitous access to enterprise IT systems throughout the global enterprise yields a more productive and efficient workforce, allowing employees to access resources without being tethered to a traditionally static wired network connection.

Since the introduction of IEEE 802.11 based WLANs, many documents have evaluated the Return on Investment (ROI) and cost/benefits of deploying WLANs across horizontal market segments. One document in particular, released by the Wireless Local Area Network Association (www.wlana.com), found that the average ROI of WLANs was 8.9 months. A recent independent study by NOP-Technology World found that the annual estimated ROI of a WLAN is \$7,550 per employee: the result of both cost savings and productivity gains. Such documents underline the many advantages of WLANs. To ensure that these advantages – and the corresponding ROI – are realized, it is important to examine and evaluate a number of key issues before implementation. The following document – prepared by Signa Services, a hardware-neutral WLAN educator and professional services organization – examines these issues.

The Existing Network Infrastructure

While the majority of network topologies and protocols in use around the world today are both Ethernet based and utilize a TCP/IP protocol stack – the most readily supported configuration by most WLAN vendors – a thorough examination of the existing wired infrastructure is warranted. The attractiveness of WLANs has always been the ability to augment or supplement existing wired LANs in difficult-to-wire locations. However, wiring remains a consideration when deploying WLANs, as the infrastructure must be extended to the system's access points. Subsequent access points may be deployed wirelessly via a wireless distribution system (WDS), however this configuration too must be carefully considered. Cabling is also very important if you're planning to deploy Power over Ethernet (PoE) functionality. This feature allows for both data and power to be delivered via Cat5 cabling, doing away with the expense of delivering AC power to individual access points that may be in difficult to reach places. This ultimately results in lower deployment costs. If you're planning to deploy a system that incorporates PoE you should be aware that this renders a WDS impossible. Thus it's important to carefully examine the different benefits of these configurations before making a decision.

Based upon a sound business case to implement a WLAN, an organization must also be aware that the system will never behave or perform precisely like the wired network. For example, wireless Ethernet (CSMA/CA) differs from wired Ethernet (CSMA/CD) in their access methods. Another example is TCP/IP: its inherent back off algorithms will actually degrade the performance of wireless clients when attempting to retransmit lost packets. Understanding how a WLAN and its clients will perform will allow an organization to better design and implement a viable and feasible wireless networking solution.

The proper extension of technologies and corporate policies to the wireless clients (i.e.: security policies, like RADIUS and VPN) must also be examined.

Segregation of the wireless clients, often referred to as compartmentalization, helps with performance issues as well as administration and troubleshooting.

Multi-Site Consistency

Today, many companies have global offices with a globally mobile workforce. The WLAN setup must reflect this to ensure ease of use for the mobile workforce. If settings remain consistent throughout offices, users will be able to seamlessly connect to enterprise-wide resources with little to no re-configuration down time. Not only will mobile workers experience less down time, IT staff will be relieved of technical support requirements when mobile workers enter remote offices. This should be considered for remote offices, home offices and remote dial in access to a corporate network. As more and more workers request wireless networks at home with a direct link into corporate networks, IT staff need to ensure settings and configurations are similar and thus transparent to the worker.

Mobility and Roaming

Mobility is why companies go wireless. And yet many discover that the wireless coverage is inadequate or hampered by "dead-spots". A site survey – explored in a later section – can help to minimize and even prevent this. However, the restriction of mobility is always a possibility with wireless networks. Many IT personnel are unaware of the limitations posed when roaming workers cross over subnets. More important, some of today's security solutions do not *permit* users to cross over subnets or even to leave a specific coverage area. Consequently both standards based and vendor specific roaming capabilities must be closely examined. In larger campus type settings, IP addressing and user mobility across various network segments will become increasingly important. Employing a robust security solution will also become increasingly complex. It is therefore critical to partner with a WLAN provider that is highly experienced at providing robust mobile solutions with the required built-in security.

Access Point and Wireless Client Management

Vendors have packaged their products with utilities that not only address the site survey, but manageability and administration of the WLAN. Just as critical is the value of pre/post sales support and the specialized expertise and skill set that an organization can provide. When deploying a WLAN, look to partner with a company that can support the entire wireless infrastructure, including services such as a 24/7 help desk, remote administration capabilities and RF diagnostics.

Of particular concern is – in certain applications – vendor specific utilities and specs may not be applicable. For example, when deploying a WLAN in a public area such as an airport, a vendor specific utility may not work for all clients because travelers will not all have the same product. Consequently, generic wireless characteristics need to be retrievable and monitored. This is a very important issue for administrators and service providers.

While wired and wireless Ethernet differ in their access methods, administrators should expect the same degree of manageability from wireless networks as wired networks. The software that an administrator uses to manage the wired network should also lend itself to managing the wireless network. This allows the enterprise to standardize the management platform. In addition, the ability to manage, upgrade, and configure groups of access points and clients greatly simplifies WLAN administration. Organizations should thus ensure that the WLAN allows this functionality.

While the WLAN architecture will vary between small, medium and large installations, a controller-based architecture should also be considered. This controller can take the form of hardware that sits on the network or software that is loaded onto a resident server within the network. These products not only deliver value added functionality such as Mobile IP, and robust security offerings, they deliver a method of manageability and administration.

Wireless Card Interoperability

802.11b cards from various vendors can provide very different range limits. Access points may provide coverage to one client and deny it to another in the same location. This is the result of the basic radio frequency (RF) performance of the radio's transmitter/receiver. Some vendor radios can boost their power for greater coverage performance. For this reason, the location of access points may differ between public and private implementations. In the case of a campus environment, where both the access point and client wireless network interface card can be ensured and standardized, the coverage and performance / bandwidth is constant.

Many are unaware that features over and above the IEEE 802.11b / 802.11a standard, such as EAP Security, are not interoperable among different vendors. In addition, features such as load balancing will not work with a mix of client radios. It is therefore important to differentiate between the 802.11 standard and vendor proprietary features. Because many WLAN installations are based on the features and functionality of the infrastructure products (access points) it's important to ensure

that the vendor's client radio can be made available in a wide range of clients, from notebook computers to PDAs and inventory tracking handheld terminals. This is not always the case.

Beware of creating a "closed system" which will lock the WLAN into a vendor specific solution. This is particularly problematic in public areas, where various radios will be present.

For the most part, products that have obtained Wi-Fi certification will, at a minimum, guarantee a basic level of interoperability.

Security

While in recent months the security offerings inherent in 802.11 based products have experienced a great deal of criticism due to their vulnerabilities, some basic security offers should be employed: ESSID, Packet Filtering WEP 128, and MAC Control List.

As discussed earlier – traditional wired networking security policies must also be ported to the wireless infrastructure. While Signa does not endorse any one particular solution, there are several enterprise standards, like EAP, RADIUS and VPN, available from a number of vendors. Again, security solutions may differ depending on control over the client card deployment.

Site Survey

The site survey (SS) is of paramount importance to the success of the WLAN implementation. A SS can provide details about coverage and bandwidth performance at different locations within a cell. It also indicates where access points should be located. Access point density will increase if an all time 11Mbps coverage area is required: a properly completed SS will clearly indicate where the fall back data rate of 5.5, 2 and 1Mbps areas are.

A great deal of information can be obtained from a SS: even more important is how that information is analyzed to support the following: cell planning; cell search threshold; range and throughput; interference/delay spread; bandwidth management for applications like voice over IP; access point density and load balancing.

Surveying for the "weakest link" is another important activity. This requires a consideration of different radio cards (discussed earlier), as well as the devices themselves and how they house the transmitter/receiver (radio). For example: surveying with a laptop with an exposed radio will not accurately illustrate the coverage that a traditional AIDC terminal will experience. This enhanced performance also holds true for clients that utilize antenna diversity.

With the limited channel availability, channel usage and selection are paramount. It isn't simply a question of installing more access points to provide more performance or greater coverage. The limited channel capacity of 802.11 based WLANs does not allow for an infinite number of access

points and overlapping coverage within a given area. To optimize the WLAN, work with providers that have an intimate understanding of the behavior of radio frequency and wireless standards. This becomes even more important when deploying dual radio access points.

Antenna Selection

Antennas deliver flexibility and robustness to any WLAN. Hardly referenced when discussing WLANs, it is the antenna that optimizes certain applications – such as building-to-building bridging. Because wireless is a very dynamic medium, we can – by utilizing high or low gain antennas – alter how the signal propagates. This in turn focuses an RF pattern and energy down a long narrow hallway rather than into walls, which would waste energy and/or cause multi-path interference.

It should also be noted that antenna diversity offers substantial benefits to a WLAN implementation, providing the luxury of more than one antenna and the ability to select the best antenna for usage. Implementing antenna diversity requires detailed knowledge of RF properties and how the antennas should be deployed. Antennas placed too close to one another will actually cause degradation of the RF performance as opposed to helping it. Utilizing antenna diversity will also have an impact on how a site survey is performed and its results.

The design, implementation and support of wireless networks is an extremely specialized field. It requires an in-depth understanding of the special challenges of this technology – just some of which are explored in this paper. The ability to identify and effectively address these challenges can mean the difference between a successful WLAN implementation and one that fails to deliver the expected benefits and returns on investment.

About Signa Services:

Signa Services is a member of the Psion PLC Group of Companies. Its global network of wireless local area network professionals provides WLAN professional services to clients around the world. Signa leverages the experience and expertise of Psion Teklogix – a Psion PLC company that has developed leading wireless solutions for industrial environments for more than 20 years. Signa Services is a hardware-neutral WLAN professional services organization with a long-standing track record of performance and innovation in the wireless network industry.

