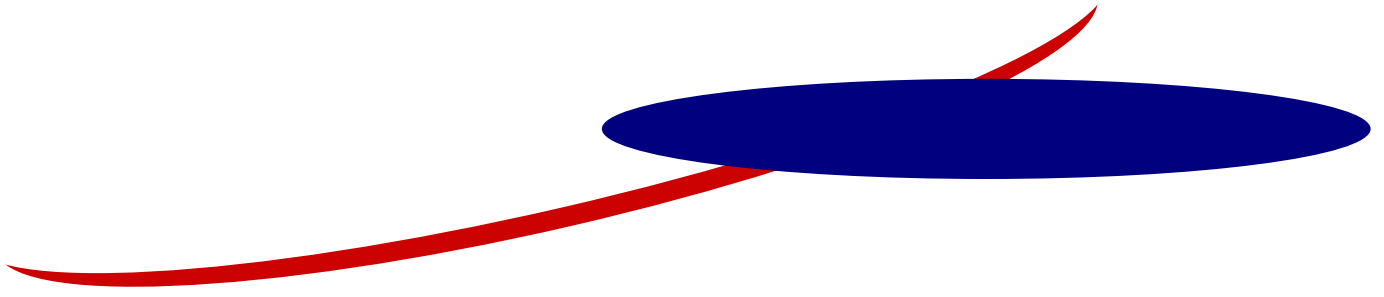


WIRELESS LAN DEPLOYMENT

Deploying
Wireless
Networks

A Datanamics Labs Research White Paper





DEPLOYING WIRELESS NETWORKS

An Overview of Analysis and Planning

By Bill Fearn

“...more convenient and productive...”

During the last few years, an increasing number of wireless products have hit the general market. Because of their low cost, convenience, mobility, and interoperability there are now more instances where wireless networking becomes an option in the corporate wired environment. This white paper is one of three produced by the Datanamics Labs™ development team to assist in dealing with technology, deployment, and security.

Corporate IT may decide to add a wireless network into the existing infrastructure for competitive or economic reasons. Extending the network into a new office may now be more cost effective if implemented with a wireless network solution. Building to building network connections may be more cost effective with wireless bridge solutions versus trenching for a permanent cable. If employees use wireless access on the road, it might be more convenient and productive for them to have wireless access when they are back at their home office and in areas of the building that do not have conventional network access such as the lunch room or outside campus areas.

Computer users are starting to purchase and “experiment” with wireless devices on their own and are beginning to use them with their business computers. With the advent of numerous commercial and free wireless “hot spots” now found in airports, hotels, coffee shops and other commercial establishments, wireless LAN cards in notebook PC's and PDA's are becoming extremely convenient. Homeowners are setting up small wireless networks rather than wiring their homes for Ethernet. Since wireless LANs are difficult to design, and the security implications are greater than a wired network, the first step of deployment should be to determine the need.



“IS managers should start now to assess the need for bringing wireless devices into the network and gain a basic understanding of some of the design considerations of a wireless network.”

I. Determine the Need

It is apparent that the proliferation of wireless devices will certainly increase, so IS managers should start now to assess the need for wireless devices in their networks and gain a basic understanding of some of the design issues. Ask yourself, “Is there a real business case for bringing wireless networking into my corporate environment.” There may not be a compelling reason. Initially, wireless networking may have been brought into the office because someone thought it was “cool” and just had to have it. If that is the only reason you can find, don’t think further about deploying a wireless network. As a matter of fact, you should probably remove any ad hoc Wireless Local Area Networks (WLANs) that may have been set up on your network. They can be fraught with security issues. It should be noted that currently, the 802.11b or Wireless Ethernet Compatibility Alliance (WECA) compliant system has a relatively low security rating out of the box. The Wired Equivalent Privacy (WEP) security provided is not turned on by default, and even when activated, has been shown to be fairly easy to break. However, once a need has been determined, focus next on the site survey and careful planning.

II. The Site Survey

“A reputable firm experienced with wireless site surveys and installations should be consulted.”

The site survey is critical to the design of a wireless network. A reputable firm experienced with wireless site surveys and installations should be consulted. Provide the consultant with as much information about your existing wired network and your plans for the wireless network as possible. For the wired network you should have: floor plans, wiring closet locations, Ethernet and electrical wiring diagrams. In commercial buildings and warehouses there are many kinds of equipment that can emit radio frequency in the same general bandwidth as WLAN devices. Engineering diagrams showing locations of microwave ovens, satellite systems, wireless phones, etc. are very important. There is a new technology called RF lighting that could also be a factor. Its use in the same environment considered for wireless access should be identified and avoided. For the wireless network you need to identify for the surveyor how many total users will require wireless access, their





maximum density in a given area, and where they will require that access. It is then possible to produce a comprehensive strategy for deploying the wireless network.

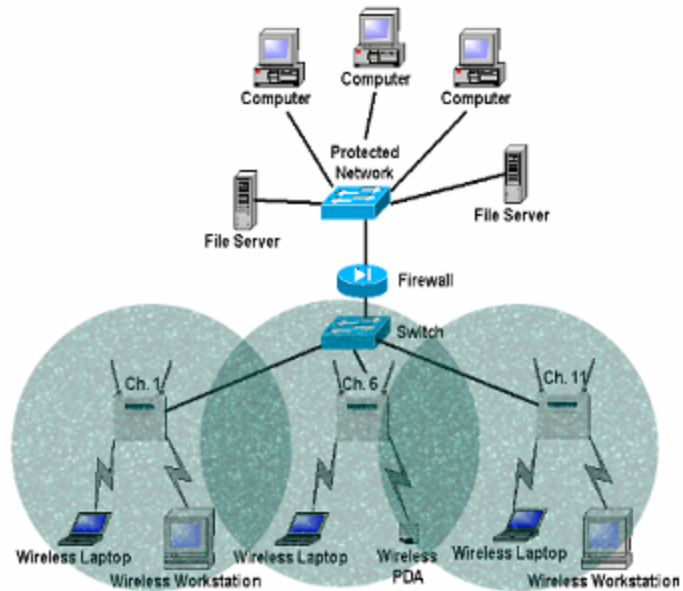
Once this information is gathered, a site survey can be conducted. The site survey should keep in mind two distinct design features when integrating the WLAN into the existing wired network. How access points connect to the wired LAN is one design consideration. The other is the correct placement of access points to provide the most efficient coverage and maximum bandwidth to the required users.

III. Connecting to the Wired Network

“If the data found on the WLAN needs a high degree of security, then how access points connect to the wired network becomes extremely important.”

Let us first take a look at how access points should connect to the wired LAN since it is often overlooked. If the data found on the WLAN needs a high degree of security, then how access points connect to the wired network becomes extremely important. If access points are simply connected to the nearest network switch, you may find that they are connected to separate network segments. Users will not be able to roam from one access point to another seamlessly because they will be on different IP subnets.

If all access points connect to their own network segment, it greatly enhances the ability to secure the wireless network. A firewall between the wireless and wired networks can be used to monitor access attempts and facilitate IP Sec VPN's with the wired LAN. In addition, a user roaming from one access point to another would still be on the same network segment. It is then easier to establish the size of the network segment since the number of users on the segment would be based on wireless users only. This provides the network administrator much more control over the security of that segment.



IV. Locating Access Points

In an “ad hoc” wireless network little thought is given to proper access point placement. Many consumer WAPs have a fixed, omnidirectional (in all directions) antennae that is directly attached to the access point body and therefore does not allow for any other type of antenna. Since WAPs need to connect to the wired network and require power, it is common to find them placed near a wall to get access to the wired network and a power outlet. This is a poor practice because it would result in loss of much of the signal and could present security issues since some of the signal would propagate beyond the wall to an adjacent room, occupied perhaps by an unscrupulous neighbor. Placing WAPs on cabinet tops or on other movable objects can lead to problems down the road. Furniture may need to be rearranged and along with that the WAP would need to be relocated.

“Permanent locations should always be established for WAPs...”

Permanent locations should always be established for WAPs and a variety of antenna types should be used depending on the geometry of the coverage required. Select a professional grade WAP that can be connected to different antenna types. For an



office room, choose an omni directional antenna and place it in the ceiling near the center of the room. If power is not available near the WAP location, Power over Ethernet (PoE), allowing the power needed for the WAP to be supplied by the CAT 5 cable connection is an option. Depending on the number of PoE connections, it may be advantageous to purchase switches that support the PoE standard. If there are only a few connections, there are adapters that can be used for individual cables.

In surveying an outside area for coverage, the season of the year can be critical. Summer may find you faced with a problematic wireless network because the survey was conducted in the winter and tree leaves are now interfering with your signal.

There are many specialized products available to assist with an access point site survey. Recently a number of good handheld PDA based products have come on the market. Most important to whatever kind of survey device is used is its ability to measure signal-to-noise ratio (SNR) and packet retry count as well as to identify the type of RF interference it encounters.



These measurements, along with the locations of other RF sources will dictate the design parameters to assure proper coverage.

“These measurements, along with the locations of other RF sources will dictate the design parameters to assure proper coverage.”

These measurements, along with the locations of other RF sources will dictate the design parameters to assure proper coverage.

The examples above point out just some of the issues to consider when planning for the locations of wireless access points. The proper placement of access points to provide the degree of coverage required and accommodate the number of users that will access the wireless network should be done through a survey conducted by a knowledgeable WLAN engineer.



“A properly designed wireless network should be able to provide nearly the same level of security and easier accessibility than a wired network”.

V. Summary

From the discussion above, it is clear that the proper deployment of a wireless network is essential to provide an extension to the wired network that affords the added benefit of mobility and a level of network access on par with the wired network. All wired networks that connect to the Internet have a security risk that must be assessed against the value of the data on the network. There is always a final compromise between the cost to provide a given level of security per user and the value of that data. With wireless networks the same compromise must be reached. A sound wireless network deployment can minimize the effect that compromise will have on the security of your WLAN. A properly designed wireless network should be able to provide nearly the same level of security and easier accessibility than a wired network. Careful analysis and planning are the keys to building a secure, useable wireless network.



4045 South Spencer Street
Suite B - 38

Las Vegas, Nevada 89119

www.DatanamicsInc.com

Voice | 702-697-2263

Fax | 702-697-2299

E-Mail | Info@DatanamicsInc.com