



## WIRELESS STANDARDS UPDATE Issue 6/2002

When planning a wireless LAN installation, you should carefully assess and resolve potential risks such as RF interference, poor performance, and security holes.

In this update we analyse some common risks to consider when planning and deploying a WLAN, and provide some site-survey steps, which can help you, deploy an adequate and efficient wireless coverage.

### CONTENT

<u>Page</u>	<u>Title</u>
1	WLAN deployment considerations
4	RF Site-survey steps

### **✓ WLAN Deployment Considerations**

When planning a wireless LAN installation, be sure to carefully assess and resolve risks. Otherwise unforeseen implications, such as RF interference, poor performance, and security holes will wreak havoc. By handling risks during the early phases of the deployment, you'll significantly increase the success of a wireless LAN.

#### Common risks to consider

With a firm understanding of requirements, consider the following elements when evaluating and resolving risks for deploying wireless LANs:

- **RF interference.** Devices such as 2.4 GHz cordless phones, microwave ovens, and neighboring wireless LANs, can cause damaging RF interference that impedes the performance of a wireless LAN. To minimize the risk of RF interference, perform a RF site survey to detect the presence of interference, and define countermeasures before installing the access points.

The problem with RF interference is that it's not always controllable. For example, you may deploy an 802.11b wireless LAN in an office complex, then three months later the company next door installs a



wireless LAN set to the same channels. This results in both wireless LANs interfering with each other.

A possible solution to minimize this risk is to utilize directive antennas that ensure transmit and receive power of the your wireless LAN falls only within your facility. This would limit the impact of the interfering wireless LAN. Of course you could also specify the use of 802.11a, which offers more flexibility in choosing channels that don't conflict with others.

- **Interoperability issues.** The lack of interoperability among 802.11 FHSS, 802.11b DSSS, and 802.11a OFDM causes problems in some cases. Even though these standard are all 802.11, they don't interoperate with each other. With so many standards, you run the risk of not allowing some users on the wireless LAN.

Consider a company that installs 802.11a access points throughout the facility today. This provides interoperability with 802.11a users, but precludes the operation of 802.11b-equipped user devices. Until multimode radio NICs ( see tchnical update issue 5/2002) are commonplace, you'll need to carefully consider the impacts of choosing the specific wireless LAN standard.

- **Security holes.** The potential for an unauthorized person accessing corporate information is a significant threat for wireless LANs. An eavesdropper can use a wireless LAN analyzer, such as Wildpacket's Airopeek or Sniffer Technology's Sniffer Wireless to passively receive and view contents of 802.11 frames. Of course this could disclose credit card numbers, passwords, and other sensitive information.

Avoid security risks by carefully assessing the vulnerabilities of a wireless LAN, and define effective security mechanisms based on the value of information you need to protect. In some cases, you may simply need firewall protection. Other applications may require effective forms of encryption. Of course 802.1X will also provide added security.

- **Applications interfaces.** In some cases, interfaces with applications located on various hosts and servers can bring about major problems when using a wireless LAN. A relatively short loss of connectivity due to RF interference or poor coverage area causes some applications to produce errors. This occurs mostly with legacy applications lacking error recovery mechanisms for wireless systems.

For example, a user may be using an inventory application by scanning items and entering total counts via a keypad on the scanner. If loss of connectivity occurs after scanning the bar code and before entering the count, the host-based application could log the use out without completing the inventory transaction. As a result, the



application on the host may record an incorrect or invalid value for the inventory item.

To avoid these types of risks, carefully define the types of applications the wireless user devices will interface with. If needed, incorporate solutions such as wireless middleware to provide adequate handle recovery mechanisms related to wireless LANs.

- **Unclear requirements.** If you deploy a wireless LAN without first clarifying requirements, then the wireless LAN may not satisfy the needs of the users. In fact poor requirements are often the reason why information system projects are unsuccessful. As a result, always define clear requirements before getting to far with the deployment.

For example, you may install 11 Mbps 802.11b today to support needs for a moderate number of users accessing e-mail and browsing the Web. Ten months later the organization may increase the density of users or need to utilize multimedia applications demanding a higher performing solution. The organization would then be facing a decision to migrate to either 802.11g or 802.11a.

If 802.11g products are available, the migration could simply involve firmware upgrades; however, the total capacity of 802.11g might not be sufficient to satisfy requirements. 802.11a would provide greater capacity, but would require changing access point hardware. In this case, the organization should have initially chosen 802.11a initially.

- **Product availability.** Solid requirements and an effective design significantly reduce most deployment risks, assuming the design specifies products that are actually available when you need them. The trouble is that vendors often miss projected release dates and have limited volumes when the products are first available.

For example, multimode 802.11a/b radio NICs *should* be available on the market by the end of 2002. You're incurring a risk, however, if it's crucial that these products available by then. A similar hazard surfaces if you're depending on the availability of 802.11g by a specific date to upgrade existing 802.11b access points to support higher requirements. Of course the advice here is to not totally rely on projected release dates.

By identifying and solving potential risks, you'll have a much more successful wireless LAN deployment. The key is to fully understand wireless requirements during early stages of the deployment project, identify related risks, and provide effective solutions.

Source : [www.80211planet.com](http://www.80211planet.com) / Jim Geier / May 22, 2002



## ✓ RF Site Survey Steps

With wireless systems, it's very difficult to predict the propagation of radio waves and detect the presence of interfering signals without the use of test equipment. Even if you're using omni-directional antennas, radio waves don't really travel the same distance in all directions. Instead walls, doors, elevator shafts, people, and other obstacles offer varying degrees of attenuation, which cause the Radio Frequency (RF) radiation pattern to be irregular and unpredictable. As a result, it's often necessary to perform a RF site survey to fully understand the behavior of radio waves within a facility before installing wireless network access points.

The ultimate goal of a RF site survey is to supply enough information to determine the number and placement of access points that provides adequate coverage throughout the facility. In most implementations, "adequate coverage" means support of a minimum data rate. A RF site survey also detects the presence of interference coming from other sources that could degrade the performance of the wireless LAN.

The need and complexity of a RF site survey will vary depending on the facility. For example, a small three room office may not require a site survey. This scenario can probably get by with a single access point located anywhere within the office and still maintain adequate coverage. If this access point encounters RF interference from another nearby wireless LAN, you can likely choose a different channel and eliminate the problem.

A larger facility, such as an office complex, apartment building, hospital, or warehouse, generally requires an extensive RF site survey. Without a survey, users will probably end up with inadequate coverage and suffer from low performance in some areas. You certainly wouldn't want to relocate and add access points to the facility after installing and interconnecting 20 access points or more.

When conducting an RF site survey, consider these general steps:

1. **Obtain a facility diagram.** Before getting too far with the site survey, locate a set of building blueprints. If none are available, prepare a floor plan drawing that depicts the location of walls, walkways, etc.
2. **Visually inspect the facility.** Be sure to walk through the facility before performing any tests to verify the accuracy of the facility diagram. This is a good time to note any potential barriers that may affect the propagation of RF signals. For example, a visual inspection will uncover obstacles to RF such as metal racks and partitions, items that blueprints generally don't show.



3. **Identify user areas.** On the facility diagram, mark the areas of fixed and mobile users. In addition to illustrating where mobile users may roam, indicate where they will not go. You might get by with fewer access points if you can limit the roaming areas.
4. **Determine preliminary access point locations.** By considering the location of wireless users and range estimations of the wireless LAN products you're using, approximate the locations of access points that will provide adequate coverage throughout the user areas. Plan for some propagation overlap among adjacent access points, but keep in mind that channel assignments for access points will need to be far enough apart to avoid inter-access point interference. Be certain to consider mounting locations, which could be vertical posts or metal supports above ceiling tiles. Be sure to recognize suitable locations for installing the access point, antenna, data cable, and power line. Also think about different antenna types when deciding where to position access points. An access point mounted near an outside wall, for example, could be a good location if you use a patch antenna with relatively high gain oriented within the facility.
5. **Verify access point locations.** This is when the real testing begins. Many wireless LAN vendors provide free RF site survey tools that identifies the associated access point, data rate, signal strength, and signal quality. You can load this software on a laptop or PocketPC and test the coverage of each preliminary access point location. Alternately, you could use a handheld site survey tool available from several different companies.

Install an access point at each preliminary location, and monitor the site survey software readings by walking varying distances away from the access point. There's no need to connect the access point to the distribution system because the tests merely ping the access point. Take note of data rates and signal readings at different points as you move to the outer bounds of the access point coverage. In a multi-floor facility, perform tests on the floor above and below the access point. Keep in mind that a poor signal quality reading likely indicates that RF interference is affecting the wireless LAN. This would warrant the use of a spectrum analyzer to characterize the interference, especially if there are no other indications of its source. Based on the results of the testing, you might need to reconsider the location of some access points and redo the affected tests.

6. **Document findings.** Once you're satisfied that the planned location of access points will provide adequate coverage, identify on the facility diagrams recommended mounting locations. Of course the installers will need this information. Also, provide a log of signal readings and supported data rates near the outer propagation boundary of each access point as a basis for future redesign efforts.



These general site-survey steps should guide you when planning the implementation of a wireless network. If you are not experienced in doing this you should contact your system integrator who is experienced in performing these site-surveys.

Source : [www.80211planet.com](http://www.80211planet.com) / Jim Geier / May 10, 2002