

Vol.6 Number 4  
April 2006

## In-Building Wireless: Examining Your Options

A recent report from J.D. Power and Associates states that a typical wireless customer places 40% of their calls indoors. The problem is that traditional cellular service is spotty when you're dealing with a steel and concrete environment. In-building wireless offers your employees a solution that will maintain their mobility and still give them access to the high voice quality of your corporate PBX. But with the wide spectrum of in-building wireless options available, what is the best choice to meet their needs?

To answer this, we will examine the advantages and disadvantages of using a common WiFi approach (utilizing 802.11 frequency), versus using a "proprietary" frequency set using other frequencies such as 1.9Ghz. The differences between each technology should make your selection easier as you compare their capabilities to your unique needs.

### WiFi

WiFi is the wireless operating environment that you will find in common wireless hot spots. You can install such a network, optimized for voice, within your office environment, in much the same fashion as a coffee house. As this is a common technology, handsets that you purchase for your system might be able to work in other public hot spots as well, but this is not guaranteed.


There are several disadvantages to a WiFi in-building phone network. As employees move through your office, from wireless access point to access point, the transition might not always be seamless. The result is that an employee on the move might lose a call, or have a break in the conversation.

Another issue to consider is security. 802.11 is an open frequency, and it will be possible for calls to be intercepted. Security can be added to your system, but it will involve a hardware and software investment, and the modifications might also limit your service.

### Proprietary Frequencies

A "proprietary" frequency is one unique to the technology that is being put into place. This type of approach uses your existing voice infrastructure, whether a Legacy PBX or VoIP. The primary advantage with this method is an employee can switch from one access point to another seamlessly. But the benefit doesn't stop there. If you have offices located in multiple cities, your wireless voice communications could be inter-connected through IP-campus networking. This would allow calls to be routed from one office to another.

It works this way: an employee leaves their office in Dallas and takes a flight to Chicago. Upon entering the Chicago office, the network recognizes the mobile handset's new location and automatically transfers all calls to the Chicago office. Inbound callers still



dial the same extension to reach the employee, and the employee still uses the same handset to dial out. That employee can move from office to office, from city to city, and still access of the functionality of your corporate PBX and voicemail system.

When employing in-building wireless using a proprietary frequency, vendor selection is critical. The right vendor should use voice scrambling and encryption when transmitting voice packets. That will eliminate the security concerns associated with common WiFi. In fact, this approach is so secure that it is current being used for wireless communications within Japan's nuclear facilities.

Another factor to consider when selecting a proprietary solution is the hardware and software involved. The right proprietary-frequency-based technology should deploy no more equipment than a blade for your voice servers and wireless access points distributed throughout the building.

The bottom line is that WiFi works fine if quality of service is not a major concern and the system will not be used for any voice communications of a sensitive nature. But for secure, reliable communications proprietary frequencies are definitely the way to go.