



Vol.7 Number 4  
April 2007

## Redefining Mobility: What in-building wireless can do for you

Imagine getting up from your desk, going down the hall, getting on the elevator, and stopping in the lobby. You pull a phone out of your briefcase and make a call, but it's not a cellular call. The call is going directly out from your corporate phone network from your own extension. You have the same call quality and phone features as if you were sitting at your own desk. That's the level of mobility that an in-building wireless network can offer.

But it gets better. Let's say you leave your office in Dallas and take a flight to Chicago. Upon entering the Chicago office, the network recognizes your mobile handset's new location and automatically transfers all calls to the Chicago office. Inbound callers still dial the same extension to reach you, and you still use the same handset to dial out. As you move from office to office, from city to city, you can still access the functionality of your corporate PBX and voicemail system.

If you set up the right wireless system over your corporate communications server or PBX this can all be reality. Let's examine what the options are in regards to in-building wireless, and how they might change how you do business.

### WiFi vs. "Proprietary" Frequencies

WiFi (also known as 802.11) is the common wireless operating environment that you will find in 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. The first of which is that as you move through your office, the transition from wireless access point to access point might not always be seamless. The result is that you might lose a call or have a break in the conversation.

Another issue to consider is security. WiFi is an open frequency and it is 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.

The other approach is to implement a "proprietary" frequency. This type of approach uses your existing voice infrastructure, whether a Legacy PBX or VoIP. The primary advantage with this method is the ability to switch from one access point to another seamlessly. And



if you have offices located in multiple cities, your wireless voice communications could be inter-connected through IP-campus networking with calls being routed from one office to another.

When employing in-building wireless using a proprietary frequency, you can gain access to voice scrambling and encryption technology. In this way you can eliminate the security concerns associated with WiFi. In fact, this approach is so secure that it is current being used for wireless communications within Japan's nuclear facilities.

### **Future Possibilities**

Future developments include handsets that can switch automatically from in-building wireless to another network when you walk outside. Currently, two different avenues are being pursued to make this happen.

One approach is to switch from in-building to a cellular network for maximum mobility. The only problem here is there are currently multiple cellular carrier networks in the United States that are not compatible with one another. Basically, what you get is a handset that can function in-building, but only on one type of cellular carrier.

Another option is handsets that can switch between a proprietary frequency and WiFi. That way, you can use your corporate PBX from whatever office you are located in, and make use of WiFi hot spots when on the road. This technology is currently under development and should make its way into the marketplace within the next few years.

