

In-Building Wireless: Frequency Matters

If you are tasked with deploying an in-building wireless network within your company, you may be tempted to deploy a basic 802.11 WiFi system. While this type of system is simple to setup, there are several major drawbacks in deploying what is basically a retail technology into a corporate environment.

The first challenge of 802.11 is that as employees move through your office, the transition between wireless access points may not always be seamless. Transmission lags exceeding 150ms could result in a broken or lost call. Another issue to consider is security. 802.11 is an open frequency, and it is possible for calls to be intercepted. Security can be added to 802.11, but it usually involves hardware and software upgrades. The modifications may also limit your service.

Proprietary Frequencies

Proprietary frequencies are unique frequency bands used by specific vendors that are unique to that vendor's product offerings. A quality offering will require very little equipment. The best solutions simply install a blade on your voice servers or PBX and wireless access points throughout the building.

With this type of approach, all call processing happens within the communications server or PBX. Proprietary frequencies can be deployed in either a Legacy PBX or VoIP environment. The primary advantage is that with this method, an employee can switch from one access point to another seamlessly (the switch occurs automatically, usually in about 50ms.). If you have offices located in multiple cities, your wireless voice communications can be inter-connected through IP-campus networking, with your calls being routed from one office to another without any interruption in service.

Imagine this scenario: an employee leaves his 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 the functionality of your corporate PBX and voicemail system.

Security Issues

When deploying in-building wireless using a proprietary frequency, vendor selection is critical. The right vendor will use voice scrambling and encryption when transmitting voice packets. That will eliminate the security concerns associated with 802.11. In fact, this approach is so secure that it is currently 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 the user walks outside. Right now, two different avenues are currently being pursued in this regard.

One approach is to switch from in-building to a cellular network for maximum mobility. The only problem here is that there are currently multiple cellular carrier networks in the United States, including GSM and CDMA, which uses different hardware codec. Basically, what you get is a handset that can function in-building and on one type of cellular carrier only.

Another option is handsets that can switch between a proprietary frequency and 802.11. That way, an employee can use their corporate PBX from whatever office they are located in, and then 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.