The Challenges Of Wireless Network Design

Today, MDU residents demand wireless access for their mobile and not-so-mobile devices. This cautionary tale of a wireless network installation gone awry shows why network designers and property owners must communicate about their objectives and develop appropriate design standards.

By David Daugherty and Clinton Cory ■ *Korcett Holdings Inc.*

A property we'll call "the Shadows" is a brand-new student housing community with about 750 beds. It incorporates all the latest amenities, including an assortment of government-sponsored energy management technology. It also contains a typical range of wireless noise generators, including resident wireless access points, microwave ovens, wireless telephones and wireless power meters.

The history of the Shadows illustrates the challenges of working with wireless communications, which has all the complexity of traditional wired networks along with such wild cards as signal strength, radio interference and additional overhead. Unfortunately, there was little or no systemic review during the design stage of how the planned property amenities would interact. The designers made no provisions for attaching third-party devices, such as security cameras or sensors for managing appliances.

Because there was little or no review in the design stage, designers made no provision for attaching devices such as security cameras or sensors.

Thus, two significant and unexpected problems had to be resolved after the network had been installed and students had begun moving in – at the same time that the developer was rushing to complete the installation of amenities. The first problem developed as the contractor began installing environmental controls to the network. Because network designers had had no advance knowledge or warning that additional devices would be attached to the network, a Dynamic Host Configuration Protocol (DHCP) conflict arose between the environmental control system and the wireless access points – that is, multiple devices had the same IP address.

IP address allocations for a residential network are based on expected usage of resident devices, so when a third party installs additional devices that require IP addresses, the number of IP addresses falls short. Additional address space must be obtained and deployed to cover this unexpected addition to the network. In the meantime, managers must shut down the third-party devices or tolerate users' being affected until additional IP space is obtained and deployed. In this case, residents were very irritated for several days until the problem was identified and corrected and service levels returned to normal.

From a network design and performance perspective, this was a normal experience. From a property operations standpoint, however, this kind of oversight can significantly impact the reputation and subsequent business performance of a new development.

About the Author

David Daugherty is the founder and CEO of Korcett Holdings, and Clinton Cory is the senior network engineer. Korcett Holdings (www.korcett.com) is dedicated to the development and deployment of next-generation managed service solutions.

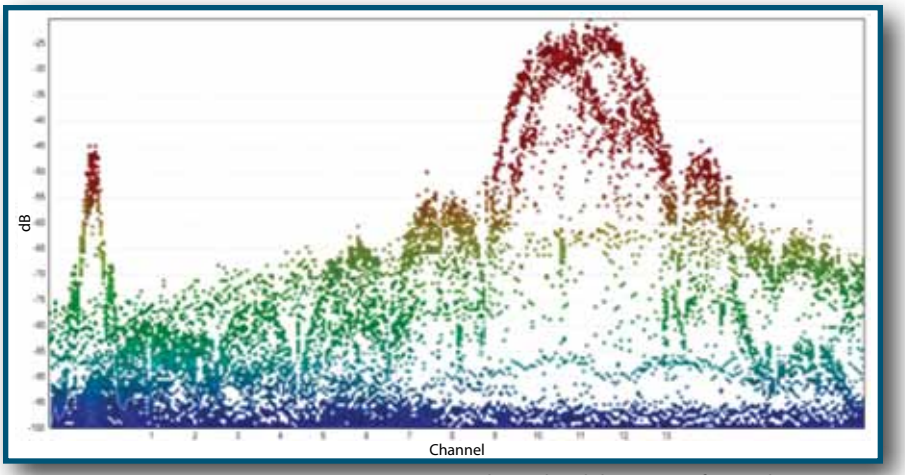

Figure 1: ZigBee transmissions are in a separate channel and do not interfere with Wi-Fi.
Legend: red = strong; green/yellow = moderate; blue = weak

Once the DHCP conflicts were resolved, a more serious issue arose: The environmental control system began creating wireless interference. The sensors in this system used the ZigBee wireless protocol – a low-cost, low-power, wireless mesh network standard. ZigBee's low cost allows the technology to be widely deployed in wireless control and monitoring applications.

In this case, the ZigBee devices had been improperly configured during manufacturing and were transmitting continuously. To compound the problem, these devices were installed in close proximity to the units' wireless transceivers. Because ZigBee devices normally operate at low power and transmit only in short bursts, they were not immediately identified as the problem. Wireless performance problems therefore continued for weeks before the problem was properly identified and resolved, resulting in a rash of unfavorable social networking posts by irritated student residents.

Figure 1 shows transmissions by ZigBee and channel 11 Wi-Fi devices. The ZigBee device signature is the sharp peak near the left of the illustration. The channel 11 Wi-Fi device has the dome-shaped signature further to the right.

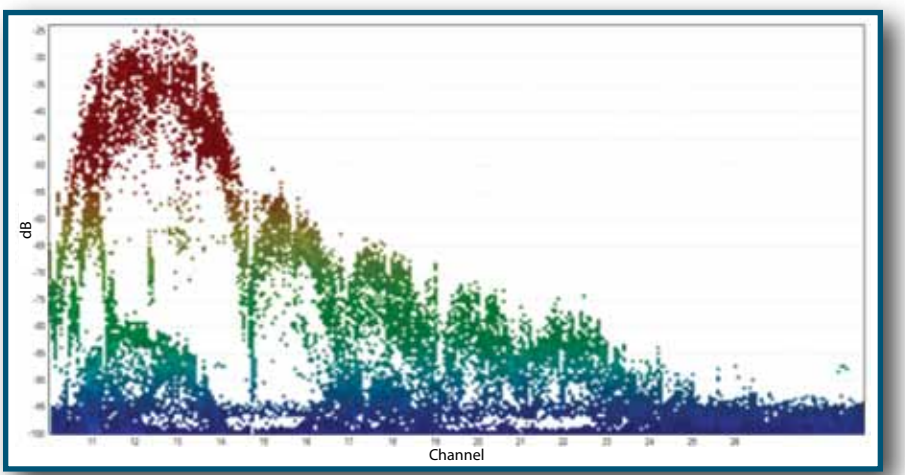

Figure 2: Here, the ZigBee signal is interfering with the Wi-Fi signal.

Figure 2 illustrates the disruption caused when an access point and a ZigBee device compete for the same wireless spectrum. The ZigBee signal can be seen under the wireless access point signal at the left.

This is where the discussion gets interesting. Because the network designers did not completely understand the operational objectives for the property, they failed to anticipate these network performance issues. Instead, under pressure from the property developer to reduce capital costs, they selected a lower-cost wireless access point. If the network designers and developer had invested a bit more time during the planning stage, they would have used a more robust wireless technology and avoided most of the residents' complaints.

The bottom line for the Shadows is that the cost of identifying and correcting the interference problems far exceeded the cost of using more expensive wireless access points. The cost was compounded by irritated residents' expressing their displeasure on social networking channels.

To reduce capital costs, network designers selected low-cost wireless access points. Using a robust wireless technology would have avoided problems.

The long-term cost of such a public failure will be difficult to assess in such a hotly contested market. In the end, there was no excuse for not using more robust wireless network technology – a mistake the developer probably will not repeat.

In the next issue, Metrics will look at the underlying wireless network standards and the relationship between antenna design and network performance and then present a set of usable MDU design considerations, including a recommendation for future-proofing wireless designs for three to five years. Those who can't wait for the next installment should contact Dave at david@korcett.com. ❖