

PROCESSOR.

Deploy A Wireless Infrastructure

Get A Grasp On Building Layout, Business Objectives & Employee Needs

Key Points

- Plan out who will be able to access the wireless network and evaluate why they need access.
- Consider the security variables, especially for guest access and employee access to applications.
- Examine building floor plans and determine where access points should go.

For most IT deployments, the more you know about the technology, the better. With a wireless infrastructure, there is a lot to learn about Wi-Fi radio technology, networking backhails, and security protocols that can protect company assets and keep your network safe. But a thorough knowledge of the building layout, nontechnical needs of employees—such as whether they typically need to connect in a cafeteria or in a conference room—and a good understanding of business objectives also come into play during deployment. For some SMEs, this might mean setting aside any conceptions of how ubiquitous a wireless network needs to be and understanding that an “all or nothing” approach usually will not work, especially using the current wireless standards.

■ Planning & Preparation

As with any major roll-out, a wireless infrastructure—one meant to provide easy access to the Internet from laptops and smartphones or one that provides wireless access to business applications—requires careful planning and preparation. According to David Johnson, co-founder of and consultant at The Fulcrum Group, planning for a wireless deployment means determining an appropriate level of access for employees and deciding on how to provide guest access.

“Internal office workers may need access to IT systems, and you may have guests who simply need to get on the Internet,” says Johnson. “There are other types of users, such as vendors and strategic partners, who need a separate level of access. The first thing we usually cover with our clients is who needs to access what and what they need to access.”

Cameron Niles, CTO at IT consulting company Syzygy 3, agrees that planning the “who and what” is important for the ever-changing IT landscape. Companies might need to provide access to more than just laptops and smartphones and should plan for employees with IP phones (such as those that use Skype or another VoIP provider) that use a greater amount of bandwidth. Niles says different user groups have very different needs: Some require very fast access to applications, and others just need to check email occasionally in an entryway.

According to Niles, one trend in many companies is to deploy two separate wireless networks, one for internal use and one for guests. This points to the fact that an SME

needs to plan for how employees and visitors will use the network and also addresses another initial deployment concern: security.

For many enterprises, the two-network approach solves this problem, and Niles says that in some cases, a wireless deployment will involve a completely separate switch that will be used for the “public” wireless access and then a separate wireless controller that is used for making sure a private company network is secure and not even accessible for guest use. With a wireless controller used for deployment of a private company Wi-Fi network, there is less danger of a hacker in the parking lot tapping in through a widely available access point and stealing company information.

Wireless security is also directly related to compliance, says Mark Coltharp, a technology solutions consultant for Accuvant.

“Every SME thinking about a wireless deployment should determine whether or not it must comply with industry regulations or standards such as the Health Insurance Portability and Accountability Act (HIPAA) or Payment Card Industry Data Security Standards (PCI DSS),” says Coltharp. “SMEs should also look at the current infrastructure that’s already in place for networking and end computing devices to evaluate how compatible the network is with wireless infrastructure and industry standards for wireless.”

■ Building Considerations

Interestingly, after planning out who will access the network and resolving security issues, the next step in the process is not necessarily IT-related and involves taking a close look at the building structure. This may require assistance from a facility management team or require that you examine building blueprints. According to John Jankowski from JanCom Technologies (www.jancom.com), building considerations are critical to the success of a wireless deployment because it is often difficult to know whether a wireless signal can reach one particular room or if there is a firewall (the kind that is reinforced for a fire, not the security device) that could block a signal.

Jankowski says examining a building takes time and thought but can also be an intuitive process of just walking around the building and deciding where access points should be placed for high-traffic areas, whether there are outlets available or if the network switch supports Power over Ethernet, and whether certain groups in the building have a greater need for wireless access than others.

One important step in the process is to realize that the wireless network will likely not cover every cubicle and every desk. In fact, Jankowski says you should concentrate on areas that meet a specific need for remote access. He says the high-traffic areas, such as a conference room, may even need multiple access points, whereas a group in another corner of the building may not need access.

■ Helpful Tools

Many of the best wireless networking companies offer a bevy of tools for helping in wireless deployment. These tools can provide a basic knowledge of how access points will interconnect and any need for wireless backhaul to handle congestion. Jankowski notes that, unlike a wired network where each user connects into a server through a separate connection, a wireless network is automatically a choke point because of how a wireless network allows multiple connections that feed into a switch. Software tools—which might feature data visualization techniques—can help determine where congestion might occur.

That said, even the best software tools, which are sometimes designed only for specific kinds of deployments, cannot replace a good planning stage that examines specific building issues and addresses how the company will resolve wireless congestion issues that may arise.

Once a plan is in place, the next step is to choose the products and technologies that match the needs of the company as well as the overall plan for where you will deploy access points. Once the products are selected, the deployment phase can begin, followed closely by monitoring the new wireless infrastructure and providing maintenance to address any wireless access problems. ■

by John Brandon