All signs point to the enterprise of the future as being one in which every laptop, handheld device, and desktop PC is connected wirelessly to the corporate network. Today, enterprises are rapidly deploying in-building wireless networks based on standards such as 802.11b, which offers constant access to enterprise intranet, extranet, and Internet data and services. Compared to traditional wired networks, in-building wireless networks offer mobility, giving users access to enterprise data anywhere and anytime; flexibility, reducing deployment and network reconfiguration costs; and convenience. Within the workplace, these innate benefits foster a mobile workforce that can collaborate more easily, be productive within flexible office configurations, and travel between buildings in a campus environment or across office sites worldwide. Consequently, wireless LANs have become the preferred method of connecting users within the enterprise environment.

Like any new network access technology, wireless LANs raise new concerns, the greatest of which is security. Network managers must ensure that new vulnerabilities are not introduced to the corporate network when a wireless LAN is deployed. At the same time, they must ensure that wireless transmissions are safe from eavesdropping. Finally, while enforcing security, network managers must preserve the simplicity, ease-of-use, and performance promised by the wireless LAN; when faced with burdensome security procedures, end users will naturally seek ways to simplify their use.

At first glance, the security challenge seems insurmountable. In response, some network managers have suggested that the best way to address such concerns is to simply remove the wireless LAN. Unfortunately, this is an impractical approach; end users will continue to demand the convenience and productivity afforded by wireless LANs. Instead, network managers need to deploy layered solutions that systematically address the security issues.