For most organizations, limited wireless local area networks (WLANs) started out as a convenience — a simple way to let guests have an Internet connection while doing business onsite. Now, WLANs have become a critical resource for both staff and guest users. Staff members are using an increasing number of wireless devices — notebooks, smartphones and tablets as tools to read e-mail, manage contacts and calendars, and carry documents.

BYOD is no longer just a hot buzzword. Everyone from the top down wants the ability to be productive, whether they’re in the office or on another continent — and they want to use their own mobile devices.

In addition, staff and visitors working or attending meetings need secure and effective guest Internet access. They must be able to connect to their own networks to retrieve and share information as well as to collaborate with the organization’s users.

**ASSESSING THE SITUATION**

Growth in the need and demand for wireless services has highlighted the often ad-hoc nature of how wireless networks have been deployed in buildings and on campuses. Network managers with meticulously designed and managed wired LANs are discovering that their wireless network’s Quality of Service (QoS) doesn’t match what users have come to expect from wired networks.

As increased usage puts stress on organizational wireless networks, staff members are discovering — and voicing concerns about — bandwidth bottlenecks, performance problems and coverage dead zones.

Management and security concerns are also driving technology and systems security managers to take a long, hard look at both their wireless and wired infrastructures. In the current computing environment, users tend not to differentiate between wired and wireless access. Security policies and technologies, therefore, need to bolster protections at the point where users connect to the organization’s systems and monitor the network infrastructure — no matter how those connections are made.

**DEPLOYING AN ENTERPRISE-CLASS INFRASTRUCTURE**

To build an enterprise-class Wi-Fi network, an organization should follow a five-step process.

**STEP 1 // IDENTIFY REQUIREMENTS**
Defining the needs of the organization’s Wi-Fi networks begins with addressing two critical areas: coverage and security. Coverage defines where the wireless network will work and how fast it will operate. Security defines how users will connect to it and what access controls will apply to different types of users.

Setting the coverage parameters is not a simple matter, because different wireless uses require different types of coverage. For example, a wireless network that supports Voice over IP (VoIP) will need to

**THE RIGHT TRACK TO Wi-Fi**

**WHEN YOUR ORGANIZATION IS ON THE MOVE, ENTERPRISE-CLASS INFRASTRUCTURE IS THE TICKET TO SECURE AND EFFICIENT NETWORK ACCESS.**

---

83% of organizations that support a BYOD policy.

Source: “CITE Conference to Tackle BYOD Issues,” Computerworld.com, March 5, 2012
Building wireless networks requires blending systems engineering — properly tuning radio frequency, for instance — with hard-earned knowledge. Although there are many ways to configure and use Wi-Fi, best-in-class organizations should apply these strategies to get the most out of their networks:

**PRACTICE ACTIVE MANAGEMENT** // Wi-Fi networks don’t stay in top condition on their own. Good network management practices, including the regular scanning of logs and the active monitoring of devices and usage, will help identify problems before they affect performance.

**USE MANAGED WIRELESS PRODUCTS** // When considering wireless management, the network team should be careful to distinguish between fully managed solutions and those that only offer configuration control and log collection. Simply capturing the configurations of each AP and pushing changes to them uniformly is not true wireless management. Any deployment with more than eight APs will need a fully managed solution.

**PRIORITIZE USAGE** // A wireless network can reach near capacity even when no one is actively using it. The solution isn’t to prohibit casual use, but simply to make sure that mission-critical applications, such as VoIP (unified communications) or transaction processing, and professional uses get priority over nonprofessional or casual usage. By using management configuration, firewalls or Wi-Fi Multimedia (WMM), it’s possible to throttle bandwidth.

**DEVELOP A GUEST POLICY CAREFULLY** // Accommodating guest access to wireless networks is generally considered a requirement for enterprise wireless installations. Any guest policy must balance its requirements for accountability and prevention of “drive-by” connections with the goal of making guest connections simple and quick. Many vendors offer specific guest services, such as captive portals and automated guest provisioning systems that can ease the task of offering guests wireless connectivity.

**BUILD SECURITY FROM THE START** // Many techniques exist to increase overall security for wireless users, but involving security teams from the beginning will make it possible to incorporate key requirements into the architecture design and product selection phases of the project.
devices can be a significant drag on performance of the network if they are not removed or blocked.

**STEP 3 // PRODUCT SELECTION**
Many technology chiefs express a preference for simplifying acquisition costs and reducing learning curves by working with the vendor of the existing wired network. There's nothing wrong with this kind of thinking. But there are also good reasons not to merge wireless and wired networks too tightly.

Some vendors offer wireless controllers integrated into their wired-switch chassis. This type of tie-in should be avoided because it links any upgrades in either one of the networks to the other, which often increases complexity and causes unnecessary expense. This doesn’t mean that an organization must exclude wired vendors when implementing wireless solutions, but it would be wise to select products with the intention of maintaining a clear separation between the wireless and wired infrastructures.

With wireless standards continuing to evolve, asking a vendor for a nondisclosure briefing on future products is crucial before making any product selection. There’s nothing worse than buying 200 access points in June only to discover that the vendor will release a replacement AP with better capabilities in September. Spending extra time peering into vendor crystal balls is a savvy short-term measure.

**STEP 4 // INSTALLATION**
Installing wireless equipment generally involves running additional cabling; adding patch panels and Power over Ethernet (PoE) in the wiring closet; as well as testing, labeling and verifying.

Time and expense during this phase will mostly go into physical installation of APs, but other integration issues also require time to work through. Enterprise wireless services always link to enterprise directories (such as Active Directory). The network team must set up and test this connection and analyze possible failover scenarios. When including endpoint security checks in the wireless project (wireless Network Access Control or NAC), project managers should plan for additional time, vendor support and testing before setting users loose.

**STEP 5 // MANAGEMENT AND TUNING**
Once all of the APs have been installed, it’s important to conduct a second site survey to verify that the wireless network performs according to requirements. It’s not unusual to have to add or move APs to handle dead spots or other unanticipated issues.

Organizations that have never had an enterprise wireless network should also invest some time and money into an appropriate network management application. Some available network management applications incorporate both wired and wireless networks. A training class or onsite consulting can ease the learning curve.

It’s also a good idea to schedule periodic site surveys every year or so to check on overall performance.

**OPTIMIZING NETWORK PERFORMANCE WITH 802.11N**
Anyone currently considering creation of an enterprise-class wireless infrastructure should be sure to focus on 802.11n and eliminate any pre–802.11n equipment from the network in order to exceed speeds far above the old 54Mbps.

The following optimization strategies assist in boosting the performance of networks based on 802.11n:

**FOCUS PRIMARILY ON 5GHz (802.11a) BANDS**
Legacy wireless equipment often uses the 802.11b/g band, but it can be difficult to get good network performance in that band when 802.11n is deployed. For best performance, devices should employ the 5GHz band whenever possible to ensure that the higher-capacity 40MHz channels can be used and that more devices can share the radio–frequency space in a smaller physical area.

**USE 802.11n 3x3:3 ACCESS POINTS WHENEVER POSSIBLE**
Newer devices and APs coming on the market have three streams across three antennas (3x3:3). These have a top speed of 195Mbps, or 405Mbps with double–wide channels. The longevity required of APs makes it worthwhile to purchase devices that will extend an organization’s refresh cycle.

It’s also worth looking at how 802.11 ac could be integrated into your network. While it’s currently pre–standard, it leverages and optimizes the 5GHz band and will become standard in the foreseeable future.

**TURN THE POWER DOWN**
Wireless devices must share the same radio–frequency space. Additional power simply creates noise and performance slowdowns for adjacent devices and APs. A maximum power level of 50MW or lower will yield better network performance. If users report poor signal strength, the first solution should be to add another access point rather than turning up wireless power.

**BLOCK LOW–SPEED ACCESS**
Enterprise networks should block clients from connecting at low data rates by increasing the data rate use for beacon frames (the 10–times–a–second frame that every AP emits to announce its capabilities) as well as the minimum connection speed allowed. The default should be raised above not only the commonly used 1Mbps and 2Mbps, but also over the old 802.11b rate of 11Mbps. This adjustment will have the desired effect of blocking old 802.11b devices from connecting to the network and causing performance problems. Networks that have multicast applications, such as multicast video, should have their minimum data rates increased as well, but will require more sensitive tuning.