

Planning and Managing Wireless LANs

End users assume that setting up a wireless LAN (WLAN) is as simple as popping wireless adapter cards into their laptops and setting up an access point (AP) on their desks. Voila—a wireless LAN! IT managers know better, but they may only have experience with small WLANs set up for workgroups or conference rooms. Few IT organizations have experience building a wireless LAN with dozens or hundreds of APs. Designing an enterprise-quality IEEE 802.11 wireless LAN requires the same disciplined approach that network managers use for wired networks.

Architecting wireless LANs has some unique challenges. Wireless LANs are a shared media technology like the concentrators and hubs used in shared Ethernet networks. The absence of dedicated high-speed bandwidth means WLANs must be engineered to deliver the required capacity, rather than just adequate coverage. WLANs also present a control challenge: Switched Ethernet links provide a point of control for IT staff to manage and control a user's impact on the network. While APs will connect to Ethernet switches, a WLAN can not provide a fixed control point since many users will share the connection to an AP. In addition, users are mobile and do not remain associated with just one AP, introducing security and management challenges.

The Network Lifecycle

Building an enterprise wireless LAN requires a "lifecycle" approach whereby IT regularly revisits and repeats key network engineering processes to ensure smooth, ongoing operation. These key lifecycle processes include network planning, verification, deployment, management and optimization. After planning the network, the IT manager must verify its design before deploying it. Once the wireless LAN is deployed, the IT manager must perform day-to-day monitoring and management tasks. And as with most network infrastructures, WLAN designs must occasionally be optimized, returning IT to the planning stage.

Executive Summary

Plan the Air: When designing a wired enterprise, the network manager carefully plans for a connection to each user location, taking into account the employee's applications, the bandwidth required to deliver a productive user experience, and the resources to be shared among network users, such as servers, printers and gateways, as well as for network access from conference rooms and other visitor locations. To be successful, the same enterprise design discipline should apply to wireless LANs. The trial-and-error approach to the wireless enterprise is ineffective and, with tools that are being introduced to the market this year, unnecessary.

This white paper will help IT managers understand:

- The importance of a structured approach to WLAN planning and design
- The network lifecycle
- How to build a radio frequency (RF) plan
- How to deploy and verify the design
- What tools and capabilities are essential to manage wireless LANs
- How to continually optimize wireless LANs to ensure availability and performance

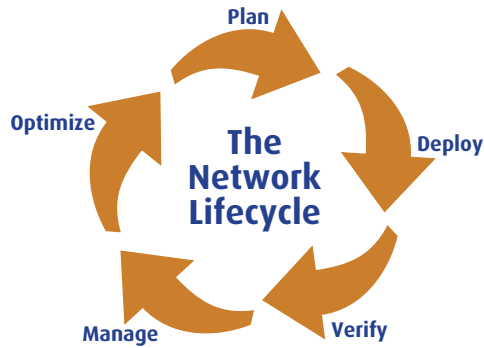


Figure 1. The wireless LAN lifecycle involves planning, deployment, verification, management and optimization.

Today's Planning Method: Trial and Error

Today, most wireless LAN designs rely on trial and error, as evidenced from the very beginning of the planning stage: the site survey. A systems integrator or network manager installs an AP and walks around the office with a wireless-enabled laptop or personal digital assistant (PDA), and site survey software to take radio frequency (RF) signal measurements at various points throughout the building. Network architects with a couple of WLAN designs under their belts have logged plenty of miles walking around facilities to measure RF signal strength and path loss levels.

Even if the network designer has the patience, time and attention to detail that's required for this tedious process, site surveys typically address only one facet of building a wireless network—the size of area the RF signal will cover. Plus, site surveys provide a one-time snapshot of the RF environment that becomes outdated as soon as the network manager walks back to his desk. A network manager has no way of knowing if engineering puts up an unauthorized wireless AP hours after the site survey is completed—until he performs another site survey or wireless users report performance problems. Along with the fact that today's site-survey tools do not consider the network bandwidth or capacity needed for enterprise business applications, which is the more important design factor for an enterprise deployment, it's surprising that any well-managed WLAN can be implemented in today's enterprise environment.

To answer the network manager's cry for help, many wireless LAN vendors bundle basic site-survey tools with their APs and network interface cards. IT organizations planning to design a large number of wireless LANs may want to purchase more fully featured site-survey software. Many site-survey tools for cellular networks also support the 802.11 standard for wireless LANs. However, these sophisticated software packages are often costly and geared toward a cellular network designer, not an enterprise IT manager.

After the site survey, the planning starts. First the network manager approximates how many APs are needed and where they should be placed, based on the data gleaned from the site survey, the office floor plan and the wireless LAN product data sheets. Then he figures out the correct channel selections to provide the maximum coverage with a minimum of co-channel interference. After that, the network manager has to fine tune the quantity and placement of APs as user feedback about application performance comes in.

This hit-or-miss approach worsens as the network gets larger. Once the wireless LAN encompasses hundreds of users, multiple floors or very large areas, it's much harder to do back-of-the-envelope calculations that will deliver a well-designed network. For an enterprise deployment, a more structured and scalable approach is needed.

A Structured Approach to Planning

The solution is to "plan the air" the way IT planned structured-wired networks. When designing a wired enterprise, the network manager carefully planned for a connection to each user location, taking into account the employee's applications and the bandwidth required to deliver a productive user experience. Additionally, he took into account the resources to be shared among the network users, such as servers, printers and gateways. The designer also planned for network access from conference rooms and other visitor locations. To be successful, the same enterprise design discipline should apply to wireless LANs.

In short, IT managers must perform traffic engineering for the wireless LAN. They must be able to start with a system design that requires a small number of APs and be able to scale it into a system with 50 APs or even a hundred APs. They need to appreciate the performance impact of having 25 or 50 users on each AP. They must know how much data users can push through the wireless network. They need to understand how the network performance will degrade gracefully with growth and at what point it will begin to degrade. Network designers wouldn't think of building a wired network without knowing the answers to these questions, and the same discipline is required for an enterprise WLAN.

Designing the RF Plan

With a structured approach, network designers create an RF plan that includes the chosen wireless LAN technology, the number of APs required, placing the APs, considering the RF loss factors, determining the cell sizes and selecting the channels. In the following section, we'll delve into each one.

First, the network designer must decide which 802.11 technology the network will use. 802.11 wireless LANs come in three flavors.

- **IEEE 802.11a.** Products based on 802.11a technology will rapidly come to market in 2003, making them more affordable and widely available. Operating in the 5 GHz band, 802.11a supports a maximum theoretical data rate of 54 Mbps, but after overhead, they will deliver throughput somewhere between 25 Mbps and to 30 Mbps in practice in normal traffic conditions. In a typical office environment, its maximum range is 50 meters (150 feet) at the lowest speed, but at higher speeds, the range is less than 23 meters (75 feet). 802.11a has four, eight or more channels, depending on the country.
- **IEEE 802.11b.** Most wireless LANs deployed today use the 802.11b technology. It operates in the 2.4 GHz band, uses three non-overlapping channels, and supports a maximum theoretical data rate of 11 Mbps, with throughput averaging in the 4 Mbps to 6 Mbps. In a typical office environment, its maximum range is 75 meters (250 feet) at the lowest speed, but at the higher speeds its range is about 30 meters (100 feet). Bluetooth devices, 2.4 GHz cordless phones and even microwave ovens are sources of interference and impact performance for 802.11b networks. 802.11b products have been shipping in quantity for several years. Pricing is affordable and suppliers are plentiful.

What's in an RF Plan?

A structured approach to wireless LANs means that network designers must build an RF plan. Decisions to make include:

- **Select the wireless LAN technology**—802.11a offers higher speeds at lower ranges, provides more channels, and is more expensive. 802.11b offers lower speeds at greater ranges, provides fewer channels, and is very cost-effective. 802.11g offers the same number of channels as 802.11b running at high speeds.
- **The number of APs required**—In an enterprise wireless LAN, architects must design for capacity, rather than RF coverage. If you plan for capacity, coverage will follow.
- **Place the APs**—Locate where the APs and other wireless equipment will go. Consider ceiling-mounting the APs and secure all other equipment in a wiring closet.
- **Account for RF loss factors**—Walls, windows and elevators will absorb signals. You must account for these factors when determining cell sizes.
- **Determine the cell size**—Using smaller "microcells" will increase wireless LAN throughput.
- **Select the channels**—Select the channels to minimize co-channel interference with adjacent cells.
- **Design in a margin**—Delay future adjustments by planning for growth at the start and by designing for greater usage than the initial deployment might require.

- IEEE 802.11g.** Offering the throughput of 802.11a with the backward compatibility of 802.11b, 802.11g operates in the 2.4 GHz band and delivers data rates from 6 Mbps to 54 Mbps. Like 802.11b, it has up to three non-overlapping channels. Backward compatibility for 802.11b means that when an 802.11b device joins an 802.11g access point, throughput for 802.11g clients will slow because of the longer transmission times to communicate with the 802.11b client.

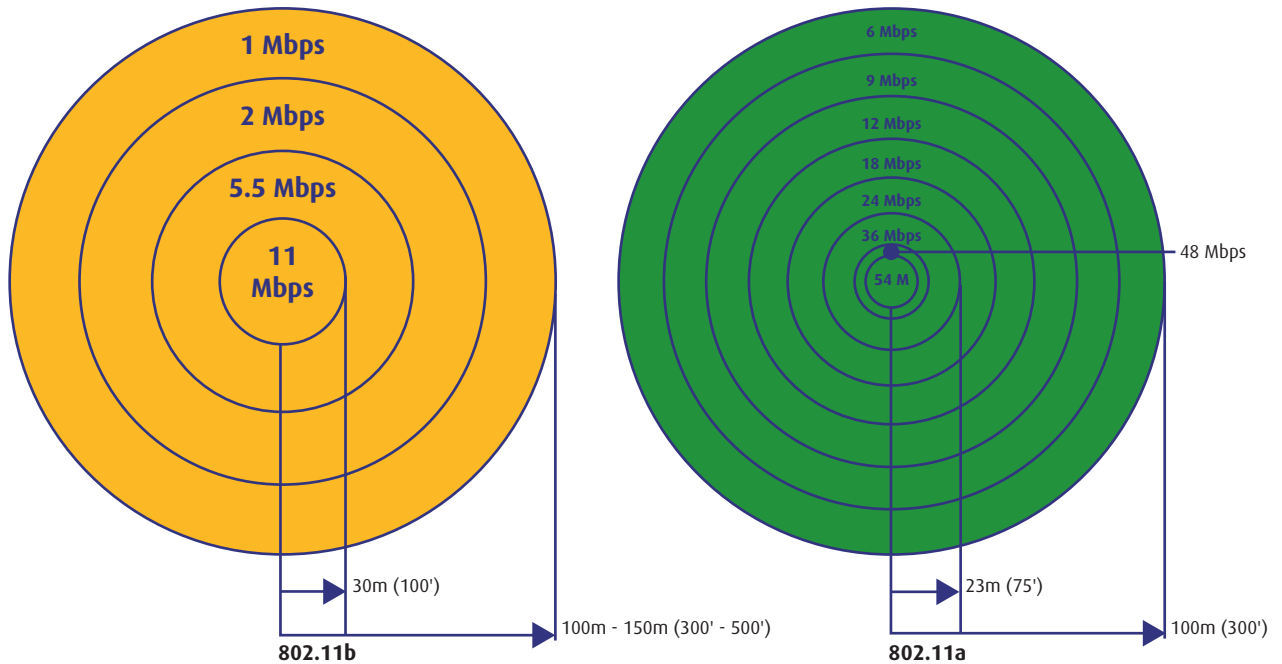


Figure 2. 802.11 association rates are highest closest to the access point. Many APs automatically decrease their association rate as the user moves farther from the access point. Network designers should consider proactively limiting the association rate to deliver a higher throughput, enterprise-class experience.

Plan for Capacity – Coverage will Follow

A fundamental requirement in designing enterprise WLANs is that you must plan for capacity, rather than focusing just on RF coverage, as designers of early wireless LANs did. In a successful enterprise deployment, users' devices must not only be able to detect the RF signal but also have adequate bandwidth to run applications effectively. By planning for capacity, you will always be guaranteed the necessary coverage.

To determine capacity requirements, the network designer must know how many users will connect in a particular coverage area, what applications they are running and how much bandwidth they will need. For an in-depth discussion of planning for capacity over coverage, see the Trapeze Networks white paper, "Capacity is Critical: Designing Enterprise Wireless LANs for Capacity vs. Coverage."

Based on the capacity requirements, the user count and the coverage areas, the IT manager can calculate how many APs need to be deployed. The greater the capacity and users, the higher the number of needed APs. A large wireless LAN may require hundreds of APs to deliver throughput sufficient for enterprise applications.

Place the Access Points

The next step is to place the APs, management controllers and any other wireless LAN components. The IT manager should locate the wiring closets nearest to the coverage areas. In workgroup wireless LANs, APs are often placed on desktops. But in enterprise deployments, APs are typically mounted on the ceiling. In addition to having fewer obstacles to interrupt the signal, ceiling-mounted APs stay above the office fray, minimizing the possibility of tampering. If the WLAN system uses management controllers, secure them in a locked wiring closet or data center.

Consider the RF Loss Factors

RF loss factors are another issue to consider. With wireless LANs, you must consider how physical objects will impact the distance that an RF signal reaches. Doors, windows, cubicles and walls all absorb and attenuate RF signals. Sophisticated equations aid in calculating loss factors, but common sense prevails too. For instance, metal walls absorb more signal than glass windows, causing greater RF attenuation.

Determining the Cell Size and Selecting Channels

Cell size is a concept specific to wireless LANs. It's defined as the area over which an RF signal from a given AP can reach. The higher the radio power in the AP, the broader the area covered by that AP. Network managers designing simply for coverage would maximize set the radio power to lengthen the signal's reach. But designing only for coverage will not provide users with an acceptable WLAN experience. To design for better capacity, network managers need to create microcells with APs.

Microcells are smaller areas of RF coverage than the AP's full power can achieve. Instead of having an 802.11a AP operate at its maximum power and achieve a cell radius of 50 meters (150 feet), network operators may create cells with a radius of 25 meters (75 feet) using a lower AP power setting. With 802.11b, a radius of 30 meters (100 feet) may be preferable to a radius of 75 meters (250 feet). Microcells boost overall network throughput by sharing more bandwidth among fewer users.

As network managers deploy more APs in a given physical part of the building by shrinking the cell size, they must carefully vary channel assignments to prevent co-channel interference. Such interference occurs when signals from adjacent APs using the same channel interfere with each other, degrading WLAN performance. 802.11a offers at least eight non-overlapping channels, while 802.11b and 802.11g have only three.

Microcells deliver greater network capacity, but they also require a greater number of channels than if the network were designed only for coverage. As the number of APs increases, channel assignment also gets complex. Again, the WLAN vendor should include tools that help managers assign channels in a manner that prevents co-channel interference.

Network managers must take care in adjusting the radio power of an AP. Too high a power level will create co-channel interference, too low will leave coverage gaps. Not all APs support power adjustments, network managers should choose a vendor who offers this feature in software to gain the needed design control. Adjusting the power levels is not intuitive; for example, changing the power from 100 to 50 milliwatts will not necessarily cut the range in half. So managers need good tools that help verify the resulting coverage area after adjusting power levels.

Specify Minimum User Connect Rates

Achieving good network throughput also requires that managers control the data rate clients are allowed to use when communicating with an AP. In order to maximize the bandwidth capacity of a particular AP's cell, a network manager must make sure that all clients connecting to the AP are running at maximum rates – either 11 Mbps for 802.11b or greater than 36 Mbps for 802.11a. Even one user communicating at a lower speed affects the throughput of everyone else because the slower user takes up more air time for packet transmissions.

Allow a Margin

A good design should also incorporate a margin for growth and increases in usage. Given the parameters of user count, bandwidth, and coverage area, managers should factor in some margin for growth so that the design is useful over a longer period of time. If a given coverage area is designed to serve 50 users, for example, the network manager may want to design for 60 users to allow for new users and users who roam into that area.

Deploy and Verify

The next step is to deploy the APs and verify the design. The greater the capacity required by the users' applications and office environment, the greater the number of APs required. Because an enterprise wireless LAN may need dozens to hundreds of APs, having automated software-based deployment tools can dramatically simplify configuration and management.

To reduce the cost and complexity associated with manual wireless LAN deployments, enterprise-class planning tools should automatically convert design plans into configuration data for APs and the other system elements. These tools should allow the IT staff to stage and deploy the system by pushing the configuration information out to all APs automatically. In an enterprise-scale deployment, it's simply not practical to configure each AP individually.

How does the IT staff verify that the wireless LAN design will work as expected? Site surveys offer no help because they provide only a snapshot of the environment at a single instance in time. Networks and offices are in a constant state of flux—users connect and disconnect in random patterns, new applications are deployed, cubicles and walls are constantly being built, moved or torn down, and people and equipment are coming in and out of the area, changing the RF environment and affecting the WLAN.

Today, the verification process consists of measuring user complaints. Users will alert the help desk that they have no network access or that an application is unbearably slow. This approach to verification clearly cannot serve enterprise requirements. Network managers must demand that their WLAN vendors bring tools to market that will automate verification. The best tools in the management arsenal will let managers double-check the planned design after they physically deploy the network. These tools should also simulate the RF topology for the user count to verify that sufficient bandwidth is available. In addition, the tools must automatically identify conflicts in channel assignments and make recommended fixes—saving the network manager hours of manual adjustments in the process. Simulation tools should also check service levels for each coverage area based on predetermined throughput and capacity parameters. If APs support load-sharing for greater performance and fault tolerance, the vendor's management tools should verify those configurations as well.

Managing the Wireless LAN

A web-based management application embedded in an AP may be fine for a 20-user deployment, but managing the WLAN AP-by-AP won't cut it for a 200- or 2,000-user wireless LAN. Nor should a wireless LAN management console break the IT budget. Today's wireless LAN management software lacks crucial capabilities for enterprise deployments.

Wireless LAN management software should tell network managers who is on the network and where they are located. It should let them set policies for users and groups of users to control what they access, what type of encryption and authorization they have, how much bandwidth they can consume, and where they can roam.

Management software should assist IT staff in configuring and managing the APs as well as help them monitor operational statistics and events. AP configuration may be a one-time event, but 802.11 technologies are rapidly evolving in every area from RF to access control to security. As a result, firmware and software updates are a foregone conclusion. A wireless LAN system should support AP software and firmware updates from a central repository. Requiring a network manager to update the configuration of every individual AP via telnet or a web browser simply does not scale.

Detecting rogue APs and users, as well as ad hoc user groups, is an ongoing requirement for intrusion detection, but today's wireless LAN management tools overlook this critical feature. Management software should detect as well as locate rogue APs, users and ad hoc user groups. After all, knowing an unauthorized user is on the premise is useless without knowing their location.

As with managing any network element, obtaining concise and meaningful statistics about network performance is critical. Reams of SNMP alerts and statistics are simply not useful, since they provide no correlation and do not help managers resolve the issue. Statistics must be collected and correlated on a system-wide basis for intelligent analysis by the IT manager. Correlation of performance data alerts IT to trends such as peak usage at specific time periods by roaming users. The trends may require tweaks to the network design for consistent service during the peak intervals.

Optimize

Optimization tools let IT staff fine-tune the RF plan based on actual performance. Perhaps users are moving around more than anticipated, so each AP must support more users. Or maybe application performance is too slow. Management tools may indicate areas of congestion; say in a hotspot area such as a conference room. Factoring in some margin for growth at the beginning of the design will help delay such optimization requirements, but ultimately network managers need optimization tools that incorporate feedback, both from users and from the system, for different areas.

With the right set of optimization tools, network managers should be able to model changes to the network. They may have designed for 1 Mbps of bandwidth per user where 2 Mbps were actually used. Optimization tools for the wireless LAN system should be able to run the calculations and tell how the network can be modified to meet new requirements. The tool should also accommodate the usual network additions, moves and changes. If the network manager wants to use the changes recommended by the management tools, then the management tools should automate all of the configurations needed for the new APs and the changes needed for the existing ones as it did for the initial deployment.

Today, few wireless LAN vendors offer optimization tools, requiring IT managers to use time-consuming trial-and-error methods. However, optimization tools are an essential part of an enterprise wireless LAN system and IT managers should expect nothing less from their vendors.

In Summary

As wireless LANs in the enterprise proliferate, IT managers must apply the same structured and scalable approach to planning and design as they do to the wired infrastructure. A trial-and-error design approach will not scale when dozens or hundreds of APs are needed. Wireless LANs are a vital part of the overall network framework and must be given proper consideration in the network lifecycle. As a result, having the right set of tools for planning, verifying, deploying, managing and optimizing WLANs is paramount to ensure a successful and scalable wireless LAN deployment.

Recommended Reading

To learn more about building wireless LANs, please read the following white papers from Trapeze Networks:

- “Capacity is Critical: Designing Enterprise Wireless LANs for Capacity vs. Coverage” white paper from Trapeze Networks
- AP Architecture Impact on the WLAN, Part 1: Security and Manageability
- AP Architecture Impact on the WLAN, Part 2: Scalability, Performance and Resiliency



5753 W. Las Positas Blvd., Pleasanton, CA 94588 Phone 925.474.2200 Fax 925.251.0642

Trapeze Networks, the Trapeze Networks logo, the Trapeze Networks flyer icon, Mobility System, Mobility Exchange, MX, Mobility Point, MP, Mobility System Software, MSS, RingMaster, AAA Integration and RADIUS Scaling, ActiveScan, AIRS, Bonded Auth, FastRoaming, Granular Transmit Power Setting, GTPS, Layer 3 Path Preservation, Location Policy Rule, LPR, Mobility Domain, Mobility Profile, Passport-Free Roaming, SentryScan, Time-of-Day Access, TDA, TAPA, Trapeze Access Point Access Protocol, Virtual Private Group, VPG, Virtual Service Set, Virtual Site Survey and WebAAA are trademarks of Trapeze Networks, Inc. Trapeze Networks SafetyNet is a service mark of Trapeze Networks, Inc. All other products and services are trademarks, registered trademarks, service marks or registered service marks of their respective owners. © 2004 Trapeze Networks, Inc. All rights reserved.

WP-PMW-501