Introduction

It’s no secret that corporations are placing greater demands on their networks than ever before—demanding support for real-time communications, for any time and anywhere access to information, and for new data- and bandwidth-intensive applications. It’s no longer adequate to have an enterprise network that cannot effectively handle the forces of change to evolve in a smart and dynamic manner.

Figure 1. HP's Wireless Product Offerings

HP offers a range of products for WLAN deployment, including, clockwise from top left, the HP ProCurve Wireless Access Points, HP ProCurve Wireless Range Extender Antenna, wireless-enabled iPAQ Pocket PC, HP ProCurve switches, HP ProCurve Secure Access products, and wireless-enabled HP notebooks.

The Internet, dynamic communications, and the mobile workforce are all changing the nature of enterprise networks. The Internet encourages an inclusive model in which organizations seek to provide users with fuller network access than they had in “traditional” data network models. The shift to digital technologies encourages a convergence of data, voice, and video conferencing technologies into a single network that supports a broad range of new applications—and implies a broad range of new users and heightened network demand. The mobile workforce and its increasingly diverse array of digital appliances increase the need for access from anywhere, at any time.

To address these and many other, related developments in enterprise networking, HP developed the HP ProCurve Networking Adaptive EDGE Architecture™, which delivers the best central command of the network with control to the network edge, to provide secure, robust functionality for current and future traffic and applications. The network edge is the place where users and applications connect, where traffic enters and exits the network, and where the network must determine how that traffic should be handled. The edge is where security policies can be enforced most effectively, where the user gains access after being authenticated by a central command resource.
Without control to the edge, decisions about security and traffic must be deferred to the network core, impacting core performance and scalability, exposing the network to malicious attack, while at the same time requiring more bandwidth in all parts of the network, driving up cost and complexity. Wireless LANs (WLANs) are one of today’s fastest-growing network technologies. Some 40 percent of businesses are using a WLAN in 2003 compared to 30 percent using the technology in 2002. Most of these organizations (70 percent) are using WLANs in departments or branch offices, but interest in enterprise-wide deployments is growing.¹

One of the key reasons for organizations to adopt the HP ProCurve Networking Adaptive EDGE Architecture is the nature of the wireless access they provide to their networks—access that must meet the demands of mobile workers, converged applications, and the open-access Internet model, while still providing the security that enterprise networks require.

This paper is a guide for getting started with WLANs. It discusses the various wireless technologies available and their pros and cons. It focuses on the planning and implementation of a site survey to determine wireless needs, including consideration of application needs, size and type of environment, and environmental factors. It presents best practices for WLAN planning, draws on HP’s own experience in providing wireless access, and gives IT professionals planning WLAN access the information they need to make intelligent purchase decisions and to facilitate their successful adoption of wireless technology.

Today’s WLAN Standards

One of the first considerations facing the enterprise that wants to adopt wireless technology is—which wireless technology to adopt? The growing range of IEEE 802.11 standards now includes 802.11b, 802.11a, and 802.11g. HP supports all of these standards.

The IEEE 802.11b standard is the most popular and widely implemented of the 802.11 family standards, for reasons including its early availability and the price of supported products. It supports maximum bandwidth of 11 Mbps—significantly better than the dial-up networking to which some users are accustomed, but far slower than other 802.11 options. This standard operates at the unlicensed 2.4GHz frequency range also used by many electronics devices including cordless phones, wireless headsets, garage door openers, and microwave ovens. That means it can be subject to interference from those devices.

The IEEE 802.11a standard provides significantly greater performance than 802.11b, upping throughput to 54 Mbps, so it can serve four-to-five times as many users as comparable 802.11b environments. And unlike 802.11b, the 802.11a standard operates in the licensed frequency range of 5 GHz and is not subject to the same interference from electronics products. Unfortunately, 802.11a isn’t a panacea. An 802.11a access point has a smaller coverage diameter, covering only about a quarter of the area of an 802.11b access point; some 802.11a devices may have a range of only 60 feet. The higher radio frequency also makes the coverage more susceptible to walls and other environmental factors. Equipment for 802.11a is also, in general, more expensive than for 802.11b. In addition to supporting this standard, HP offers turbo mode products that offer performance of 108 Mbps.

The IEEE 802.11g standard is a direct extension of 802.11b that extends that standard’s performance to 54 Mbps—the same as 802.11a. But unlike 802.11a, it operates at the same frequency—2.4 GHz—as 802.11b, so it’s backward-compatible with 802.11b access points and other devices that enterprises may already have. On the down side, because it operates at the same frequency as 802.11b, it is subject to the same interference from electronics devices as that other standard.

¹ In-Stat/MDR Information Alert, Volume #25, July 16, 2003
Because the standard was approved as recently as June 2003, use of 802.11a products isn’t as widespread as 802.11b products.

**Which standard is best?** No standard is "best" for all environments. The better question is which standard or combination of standards is best for a given deployment. Seeking this answer requires a number of other questions to be considered:

- **What is the enterprise seeking to accomplish with its wireless access?**
  Is it replacing modems and dial-up access, a relatively modest goal that can be accommodated by 802.11b, or is it replacing wired, desktop LAN access, a more intensive bandwidth goal that suggests 802.11a?

- **How many users will need wireless access and how frequently?**
  Wireless bandwidth is a shared commodity; it becomes increasingly scarce as more users access it and overall throughput drops due to contention. Sparsely populated areas, such as courtyards, lobbies, or small conference rooms, are more likely to do fine with 802.11b, while densely populated areas, such as call centers and computer labs, with more users competing for bandwidth, will do better with 802.11a. Are users accessing the network for intermittent, bursty applications such as downloading e-mail and accessing personal stores, or are they engaged in streaming or constant-connection applications such as teleconferencing? These factors clearly affect bandwidth needs.

- **How much interference exists from 2.4 GHz devices?**
  A call center, sales team, or any area with several wireless-headset or cordless-phone users will fare poorly with 802.11b. At an HP test site, for example, the use of 2.4 GHz wireless headsets by a group of users severely impacted the wireless signal strength and noise ratio in the group’s area, requiring the creation of a mixed environment with an 802.11a access point that was immune to noise from the headsets.

- **How important is interoperability of devices of varying frequencies?**
  If the enterprise has an investment in 802.11b devices and wants to keep them in service while increasing bandwidth, then 802.11g, which enables the interoperability of 54 Mbps and 11 Mbps devices, is worth consideration as an alternative to adding both 802.11a and b access points.

- **What can the enterprise reasonably expect from its wireless access?**
  The throughput rates quoted above for each standard are the optimal, theoretical performance numbers. But anyone operating a laptop on a cross-country flight knows that theoretical and actual numbers can vary. In the case of wireless bandwidth, environmental factors, security needs, and other overhead issues generally cut the theoretical numbers in half. IT teams should be prepared and be conservative in estimates of the bandwidth available from wireless access points.
Considering Coverage

Beyond bandwidth standards, another key consideration while planning wireless access is coverage—how much does the enterprise need, and where does it need it?

Complete and Partial Coverage

Can the enterprise tolerate gaps in coverage? Is 100 percent coverage the goal, or are gaps desirable? Complete coverage would seem to be preferable, since gaps can require a user to reconnect or re-authenticate. However, complete coverage comes at the price of more equipment, driving up initial costs. More extensive maintenance drives up continuing costs. Gaps, on the other hand, can make wide-spread coverage more cost-effective, if that coverage is adequate to the needs of users. As with technology standards, several factors help determine the extent of coverage needed by the enterprise:

- **Complete coverage is more important if the wireless access is replacing desktop/wired access** and becomes the sole means of network access; it’s less important if it is merely augmenting that access and users can continue to access the network via a wired connection when a wireless connection is unavailable.

- **Similarly, complete coverage is needed if the enterprise wants to enable uninterrupted roaming** down halls, through the cafeteria and conference rooms, and other spaces. On the other hand, if the goal is merely to provide wireless access in conference rooms or other specific locations, then gaps in hallways or other intermediate points may be acceptable.

- **The type of application accessed wirelessly is also a factor.** Users with devices such as HP notebook computers or iPAQ Pocket PCs may be able to roam satisfactorily through an environment with gaps if they are using only bursty applications such as downloading mail and files. If they are using streaming applications such as multimedia, or applications that must always be accessible, then complete coverage becomes more important. HP, for example, uses wireless scanners in its warehouses to manage inventory. Because the scanners must be able to transmit inventory data from anywhere in the warehouse, complete coverage is needed.

- **The enterprise may also choose not to provide coverage in certain areas,** for any of several reasons. Environmental factors in specific sites may interfere so significantly with signal strength that wireless access is impractical. Or security concerns may preclude access in some areas. If a facility is located near a hospital or other area in which wireless signals might mean life-threatening interference, such signals might in fact be against the law.

The type of coverage the enterprise seeks, complete or partial, has implications for the type of radio antennas, such as HP ProCurve antennas, it will choose for its access points. Omni-directional antennas provide a sphere of coverage with the antenna at the center. Directional antennas provide a beam or cone of coverage with the antenna at the apex and, because they are focused on specific areas, can provide longer or more extended coverage in the areas to which they are directed. Omni-directional antennas may form the backbone of a wireless site plan with widespread coverage, whether complete or partial. Directional antennas can then be used to “fill in” coverage where needed, especially where complete coverage is desired. Directional antennas can also be set to create coverage gaps in areas the enterprise wishes to keep uncovered.
In a deployment at an HP facility, the IT team was tasked with enabling wireless access. It originally deployed three 802.11b access points with omni-directional antennas. The coverage result, in green stripes, is shown below.

The initial coverage was deemed inadequate. The IT team replaced the three omni-directional antennas with six directional antennas and a high-gain omni-directional antenna. The team also raised the antennas near the ceilings, boosting radio coverage and physical security of the equipment at the same time. The results are shown below.
Capacity

Thus far, the discussion of coverage assumes that an area is either covered or not. But within covered areas, the enterprise must consider the capacity that it desires. Capacity means how much bandwidth is available for users in a particular area.

The enterprise may seek complete coverage in environments with only modest numbers of users and bursty or low-bandwidth applications. In these situations, a simple topology—with one radio serving each area on a band—may provide sufficient bandwidth. In this topology (see Figure 3) there is just enough overlap in the coverage area of each access point to facilitate roaming among the access points without losing signal strength.

Figure 3. A standard wireless LAN topology

In this example of a standard topology, eight access points, based on omni-directional antennas, each generate a coverage area with a radius of 300 feet. Three channels or bands—this example uses channels 1, 6, and 11— are required to minimize the conflicts when overlapping coverage occurs on a single band. This example hosts a moderate number of users, up to 25 users per access point or coverage circle.

In areas with high concentrations of users or bandwidth-intensive applications, a wide-coverage, high-capacity topology will be preferred (see Figure 4). In this topology, the access points are placed closer together so that the area being served has two radios covering each client location. One radio (the one closest to the client) is the prime connection point. The other provides increased capacity, but also serves as a backup which also increases availability. The radios in each pair coordinate between active and standby status to reduce interference. This model is more costly and complex than the previous model but does a better job of serving large numbers of users (40 or more per access point). Ideally, the primary and backup radio connections should be on separate back-end infrastructure elements (e.g., power grids), to minimize the possibility that both will fail simultaneously.
Figure 4. Two examples of a wide-coverage, high-availability topology

The example on the left uses omni-directional antennas as access points. The example on the right uses directional antennas.

Size Matters

Another way to begin thinking about the development of wireless access is to consider the size and type of organization in which the WLAN will be deployed. Small and medium businesses and non-profits share certain characteristics, as do various corporate WLANs and, at the high end, enterprise-level WLANs.

Entry-level WLAN Implementation

In general, an entry-level WLAN consists of single-node access point coverage of the service area, with just enough overlap between the coverage of access points to facilitate roaming between access points. Most implementations of this type find 802.11b access points to be sufficient, although higher bandwidth can be achieved using 802.11a equipment if needed. If both bands are used simultaneously, they are typically hosted by the same access point. In this case, an 802.11a radio and an 802.11b radio are housed in the same box.

The scale of this implementation is generally limited and generally consists of a single subnet. Companies generally have guidelines on the size of this subnet, the number of clients it can support, its bandwidth and loading.

Despite its relatively small size, the entry-level WLAN implementation still needs to consider encryption and authentication protocols. A product such as the HP ProCurve Wireless Access Point 520wl supports 64- and 128-bit encryption, as well as authentication by client MAC address filtering, RADIUS-based MAC address authentication, and 802.1X.
Figure 5. Entry-level WLAN Topology Example

Standard WLAN Implementation

A standard WLAN, as defined for the purposes of this paper, is considerably larger than that of the entry-level WLAN, with correspondingly higher requirements from wireless technology, including the need for wider coverage, multiple radio coverage for greater availability, multiple subnets, and higher levels of security and management. These greater requirements can be supported by equipment such as the HP ProCurve Secure Access 700wl series access controllers and access managers, and may require more than one access product per subnet, depending on wiring constraints.

In this implementation, authentication and encryption tasks are partitioned between the access points and access controllers or managers, such as the HP ProCurve Access Controller 720wl and HP ProCurve Integrated Access Manager 760wl. Where both devices are involved, the set of available services is limited to the common subset. The use of access managers enables a stronger security model than in the previous configuration. With the access manager configured as the terminal point of a virtual private network, the security model can include PPTP and L2TP/IPSec security protocols.
High-Availability

A high-availability WLAN, as defined for the purposes of this paper, is created by applying high-availability structures to the wireless network and its supporting components. This includes provisioning the wireless coverage area with two independent radio sources (two access points, either single or dual-band radio cards), dual access managers, and implementing active monitoring to enable automatic failover for clients.

Authentication and encryption services are the same as for the standard WLAN implementation.
Best Practices for the Site Assessment

Consider these best practices to ensure that the site assessment is conducted as quickly and effectively as possible, contributing to a successful plan for wireless access.

User Survey

Before surveying the physical site for wireless access needs, the IT team should survey the users. What are their needs for wireless access? What are their expectations? What applications are they using—and what applications would they like to use in the wireless environment? What traffic types (bursty versus continuous or streaming) and traffic volumes are present? How densely or sparsely situated are the users? That’s important to know since this will speak to coverage needs. Might some users be located far from likely access points? That’s relevant since performance drops off precipitously near the end of a radio’s range.

Although user expectations must be balanced against enterprise constraints, such as budget, they’re a good starting point. If user expectations cannot be met, it’s best to know this up front and to educate users to the practical limitations of the wireless environment.
Inventory of Site Elements and Obstacles

With user needs and expectations understood, the IT team is ready to inventory the physical site and its obstacles and barriers to coverage. In general, objects absorb or reflect signal strength and degrade or block the signal. Examples of these obstacles are:

- **Walls** are an obvious obstacle, but by no means the only one. The composition of the wall is also relevant. So called “wallboard” will degrade but not completely block most signals, depending on their initial strength and the proximity of the access point. Heavier construction materials, such as concrete, generally will completely block a signal.

- **Ceiling tiles** can have a dramatic effect on signal strength, particularly if they are made of material such as metal.

- **Natural elements**, such as water, trees, and bushes, are found not only outdoors but also in many lobbies, courtyards or other interior public spaces. They also degrade or block signals.

- **Coated glass** - Transparent glass generally does not degrade signal strength. But it may do so if it is coated with a metalized film or has a wire mesh embedded in it.

- **Reflection** - Objects in the environment, particularly walls, don’t always absorb the signal. Sometimes they reflect it, much as a mirror reflects light. In these cases, the reflection can be exploited as a way to extend a signal or bend it around a corridor.

- **Ceilings and crawl spaces** - Many enterprises like to locate access points in ceilings or crawl spaces to hide the equipment and to enable the signal to pass over obstacles closer to the floor—but this may be impractical if the ceiling tile will absorb the signal or where there is insufficient room to mount the unit or to do so conveniently. When putting the antenna in the ceiling isn’t practical, a similar benefit can be gained by raising the antenna closer to the ceiling, although potential leakage into floors above must be considered. Where access points can be located in ceilings, the IT team may find that these locations lack necessary power sources. In such cases, Power over Ethernet (PoE) equipment – such as the HP ProCurve Wireless Access Point 420 – which provides electrical power through the CAT-5 Ethernet cable, eliminates the need for electrical rewiring.

Similarly, placing antennas in the actual room to be covered—rather than out of sight, in an adjoining room—may be the best solution to maximize signal strength. On the other hand, a team may decide for aesthetic reasons not to place an antenna directly in the room to be covered. Also, the room may lack appropriate security; an unsecured antenna in a publicly accessible area is an invitation to vandalism or theft. When the antenna isn’t put directly in the room to be covered, the IT team typically must find ways to enable the signals to penetrate walls. Sometimes, this arrangement can be used to cover several small rooms with a single antenna. At HP, for example, the IT team deployed wireless access in one facility that included a series of conference rooms along a common wall. Instead of putting antennas in each room, the team used a directional antenna—which offers greater signal strength than omni-directional equipment—turned up the gain, and successfully transmitted the signal through the wall.

Security Considerations

The inherently open nature of wireless access—compared to the wired world—creates significant security concerns, chief among them user authentication and rights enforcement, as mentioned earlier. A site assessment would be incomplete without a solid security assessment (A complete discussion of security assessments are beyond the scope of this paper and will be addressed in future papers.). Signals may be sent indiscriminately if the access points are not plotted carefully—will those signals go into public areas that can be accessed by “eavesdropping” individuals who have not passed through any type of
The authentication process to validate their presence at the site? The site survey should identify the security status of all locations considered for wireless access.

The security solution also must control network access in different ways for different types of users who may be in the same location. Some users, such as employees, may be entitled to total or broad access. Other users, such as guests or contractors, may be entitled only to more limited access. To provide two levels of access from the same location, the enterprise can create a dual series of access points, one configured with a passcode for employees and the other, without a passcode, for guests. A more sophisticated solution, requiring only a single series of access points, includes the HP ProCurve Secure Access 700wl series products, which sit between the access point and the network, functioning as a gatekeeper, or rights administrator, at the network edge. With such a device, for example, employees can be granted access to corporate resources, and guests may be granted only access to the Internet.

The site assessment should note where guests, contractors, or other non-employee users may be located, so that appropriate security solutions can be created for those areas.

**Noise**

As mentioned earlier, noise, from cordless phones, wireless headsets, and other devices operating at the 2.4 GHz frequency of 802.11b, can interfere with an access point trying to send or receive data. The site survey should note this noise where it occurs so that mixed frequencies or other workarounds can be devised. While the addition of an 802.11a access point can mitigate noise from 2.4 GHz phones, as noted earlier, that’s not the only feasible solution. The IT team may decide it’s preferable to switch the 2.4 GHz wireless phones for phones operating at 900 MHz or 5 GHz and leave the access points operating on 802.11b. Bluetooth is another option that will minimize interference with access points, as long as the relatively limited Bluetooth range is not itself a problem for users.

**Assessment tools**

IT teams conducting their own site assessments will need the proper equipment. That equipment can be relatively simple, including an access point device of the type the IT team will later install, as well as the type of client device that will be used in production, to test the access point. That client device can be a laptop with an appropriate wireless card, a handheld device such as a wireless-enabled HP iPAQ Pocket PC, or, for warehouse or other application-specific environments, a wand or scanner. When considering access point and client devices, consider how they will work together in production. For example, because HP notebooks and access points are built with the same chipsets, they are optimized for use with each other.

The HP ProCurve Wireless Access Point 520wl is useful because its Web-based, graphical interface makes it easy to perform and view the results of a link test, an end-to-end test of the wireless link that ensures the network path is working. The 520wl’s link test monitor includes presentation of signal to noise ratio, signal strength, and noise data, as well as the number of packets at various rates (see Figure 8). Packet rate information is particularly useful in a self-survey because 11Mbps packets are a good indicator of sound performance.
Conducting the site assessment

Anyone who’s installed yard sprinklers, or considered their installation, will understand the basic principles behind conducting a site assessment: the goal is to put the access point (equivalent to the sprinkler head) in locations where it’s likely to achieve appropriate coverage (equivalent to a sprinkler effectively watering a significant portion of the yard) and then measure the result.

With the access point in a given spot, the next step is to move the client device to various locations and measure the signal strength, noise level, and packet rates produced. Take several measurements from each spot to see if the results change. Where measurements are poor, the team literally maps the obstacles causing the problem and continues taking measurements until the entire environment is mapped.

Site assessment service

An alternative to the IT team conducting the site survey directly is for the team to hire a site assessment service. The use of a site assessment service may be recommended if the team lacks experience in site survey implementation or if it is trying to survey a large area quickly or with minimal team support. The site assessment service should provide complete documentation on the survey and cover all appropriate bands. HP offers such a site assessment service. More information is available at www.hp.com/go/procurveservices.
Implementing the deployment

This technical paper has focused on issues surrounding the site survey and related WLAN planning, rather than on deployment implementation. However, it’s useful to note that in at least one respect, the deployment is essentially an extension of the site survey.

Once the deployment is implemented, a next step is for the team to go back and conduct another survey, confirming that the access points are performing as intended. Where they’re not, the team may find environmental factors previously overlooked. Or the cause may simply be overestimating the access point coverage. At this point the team can remove obstacles if possible (e.g., HP once relocated an access point around a pole that was casting an unwanted coverage “shadow”), switch the frequencies of existing equipment, or add equipment (see Figure 2).

Summary

One of the key factors determining the success of a WLAN deployment is a site assessment. It is key to a successful site assessment to understand the users needs in the environment the WLAN will be deployed. The site assessment can help identify the appropriate technology standards to apply, obstacles to avoid, eliminate, or work around, coverage patterns to adopt and amount of capacity needed.

Proper testing equipment is crucial to the success of the site assessment. The equipment should accurately reflect the access point technology to be deployed, while also facilitating easy and full monitoring of testing results.

HP ProCurve Networking offers wireless products that can be used for WLAN site assessment and deployment. In addition, HP ProCurve provides the foundation for world-class WLAN solutions by consistently delivering on its value proposition, which includes the following key elements: superior return on IT, reduced complexity, security, reliability, and flexibility.

HP ProCurve Networking has a proven track record of invention and experience that allows it to deliver an adaptive and affordable infrastructure for today’s and tomorrow’s WLAN needs.
For more information

To learn more about HP ProCurve Networking solutions, contact your local HP sales representative or visit our Web site at: www.hp.com/go/hpprocurve. To learn more about HP ProCurve wireless site assessment and installation services, go to: www.hp.com/go/procurveservices.