

Planning a Wireless Network

*Nameeta Sharma & **Nikhil Saxena

*Lecturer, Department of Electronics, Poornima College of Engineering, Jaipur – 302022(Rajasthan), INDIA

(E-mail: rattle_nameeta@yahoo.com)

**Technical Analysts, Nokia Corporation, Jaipur – 302015 (Rajasthan), INDIA

(E-mail: niksaxena@hotmail.com)

****Corresponding Author**

Abstract: One of the first considerations facing the enterprise that wants to deploy wireless networking is - which wireless technologies to adopt and when? This paper examines the three prevalent standards, 802.11b, 802.11g, and 802.11a, with an eye toward the forthcoming 802.11n standard, which promises much higher throughput than is currently available. We also look at two wireless LAN (WLAN) architectures - standalone access points and centrally controlled coordinated access points - and discuss implementation considerations that can help you decide which architectures to adopt in your environment.

To help decide which standards-based products to implement, you'll want to perform a site survey that identifies the most appropriate wireless technologies and architectures for your environment. Before delving into the more technical details, let's examine what's involved in planning and conducting a site survey. In this paper we discussed this idea.

I. Conducting a Site Survey

One of the key factors in determining the success of a wireless LAN deployment is a site survey. Before deploying or expanding your wireless LAN, you need to understand the needs of users in the current environment. By performing a site survey, you can identify the appropriate technologies to apply; obstacles to avoid, eliminate, or work around; coverage patterns to adopt; and amount of capacity needed. Your site survey should yield a network design document that describes the location of each access point, its coverage area, and the 802.11 a, b, or g channel selections for the access point. The network design document should also provide a complete Bill of Materials, indicating the WLAN equipment and supplies, infrastructure equipment and supplies to provide Power over Ethernet (PoE), and additional switch ports, and should include a vendor description of each

WLAN component.

When planning and installing a wireless network, be sure to consult with a wireless communications professional to ensure that you comply with the applicable safety and operating restrictions in your country or region.

User survey

What do users need? What are their expectations? What applications are they using? What traffic types (bursty vs. continuous or streaming) and traffic volumes are present? How densely or sparsely situated are the users? How far will they be from likely access point locations?

The workspace

Consider the space that the wireless network will serve. How will it be used? What work areas, rooms, and hallways must be supported by the wireless infrastructure? Using AutoCAD or a similar tool, create a diagram of the work environment.

Obstacles to signal strength

In general, objects absorb or reflect signal strength and degrade or block the signal. Identify any potential obstacles or impediments in the area to be served. For example:

Walls - especially if the wall is composed of heavier construction materials, such as concrete. Also note any firewalls in the area.

Ceiling tiles - particularly if they are made of material such as metal.

Furniture - especially pieces that are largely made of metal.

Natural elements - such as water, trees, and bushes - not only outdoors, but also in

many lobbies, courtyards or other interior public spaces.

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

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, and data encryption. Broadcast signals often travel into public areas that can be accessed by "eavesdropping" individuals who have not passed through any type of 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 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. In a more sophisticated solution, an access controller sits 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.

In selecting networking equipment, it is essential to choose access points that provide a comprehensive range of industry-proven security capabilities which integrate easily into any network design. Your networking equipment should provide standards-based authentication and encryption methods that satisfactorily address security concerns such as data privacy, authentication, and access control. For either existing legacy WEP-based WLAN deployments, or for new deployments that have difficulty deploying 802.1X end-to-end and therefore are not suitable for 802.11i-based link layer encryption, robust VPN encryption should be utilized.

For smaller networks that function without a centralized RADIUS server for user authentication, some access points offer built-in RADIUS authentication. Your access points should integrate seamlessly with existing authentication systems.

Signal noise

Noise from cordless phones, wireless headsets, and other non-protocol devices can interfere with an access point trying to send or receive data. The site survey should identify the sources of signal noise present in each deployment area so that the WLAN can avoid at least the already existing noise sources.

Measuring signal strength

In conducting the site survey, first make sure that you have the proper equipment. That equipment can be relatively simple, including the access points, antennas, and wireless stations that will actually be used in the deployment.

Place the access point in locations where it's likely to achieve appropriate coverage and then measure the result. With the access point in a given spot, move the wireless station to various locations and measure the signal strength, noise level, and data rates produced. Take several measurements from each location to assure consistent results.

Radiation pattern requirements and special antennas

Identify any odd-shaped buildings, corridors, aisles, and similar limitations that might affect the placement of access points and antennas. Through proper selection and placement of antennas, you can extend coverage into desired areas, overcoming physical obstacles and multipath interference.

For example, if you have a warehouse with floor-to-ceiling storage bins, and you need to enable wireless network access of wireless data collection devices such as bar code scanners or other wireless handheld interactive devices, you may need to deploy external directional antennas to focus wireless coverage between each of these obstacles.

Antennas allow for more efficient coverage for specific areas, and can help achieve desired coverage, capacity, and bandwidth

objectives. A higher-gain antenna focuses the radio's RF energy into a smaller area to achieve higher signal levels and a better signal/noise ratio. This typically yields higher data rates over the area covered by the antenna.

Whether using external antennas or antennas internal to the access point, you have to consider the physical mounting locations. Mount the access points or antennas so that there are as few obstructions to the signal as possible, and be aware of the effect that the wall or column used for mounting will have on the radiation pattern.

II. IEEE Standards

IEEE 802.11 – otherwise known as the Wi-Fi standard – denotes a set of standards for wireless LANs.

The original IEEE 802.11 standard, released in 1997, defines a common media access control (MAC) layer that supports the operation of all 802.11-based WLANs by performing core functions such as managing communications between radio network cards and access points.

Subsequent amendments to 802.11 define specific physical (PHY) layers, such as 802.11b, 802.11g, or 802.11a. The physical layer defines the data transmission for the WLAN, using various modulation schemes. The number of channels the 2.4 GHz spectrum provides varies by country according to local regulatory restrictions. The FCC defines 11 channels for use in the US; 13 channels are available for use in most of Europe and 14 are available in for Japan. The channels overlap one another, since the centers of adjacent channels are separated by only 5 MHz. As a result, only three of the channels in the 2.4 GHz band are non-overlapping. Devices that use overlapping channels within range of each other will tend to interfere with one another's operation. Interference problems are avoided only by configuring adjacent access points to operate on non-overlapping channels. The limited number of available channels in the 2.4 GHz band places an inherent restriction on the capacity of an 802.11b network. (By comparison, the 802.11a standard uses the 5 GHz spectrum, which has up to 19 non-overlapping channels depending on country regulatory rules governing use of the wireless spectrum.)

What's more, manufacturers of other devices can use the 2.4 GHz ISM band without a license, so long as the wireless device operates within regulatory limits. Interference that can affect 802.11b devices include microwave ovens, cordless phones, Bluetooth devices, wireless headsets, garage door openers, and other appliances – all of which use the same limited 2.4 GHz range.

The 802.11b standard defines a maximum data rate of 11 Mbps, which provides a realistic maximum usable throughput of about 4-6 Mbps under normal conditions. (Remember that data rate is not identical to throughput; access points must handle protocol overhead, along with management and control frames that must be transmitted at the lowest supported data rate.)

When signal quality becomes an issue, the 802.11b device uses a technique called *adaptive rate selection* to scale back the rate to 5.5/2/1 Mbps. Lower data rates use less complex methods of encoding the data. Consequently, they are less likely to be corrupted by interference or signal attenuation.

III. 802.11g

The IEEE 802.11g standard is a direct extension of 802.11b that extends the maximum data rate (signaling speed) to 54 Mbps, making it possible to serve up to five times as many users.

The higher signaling speed is made possible by using a more efficient means of transmission called orthogonal frequency-division multiplexing (OFDM). OFDM breaks a wide-frequency channel into several sub-channels and transmits the data in parallel. 802.11g provides a realistic maximum throughput of about 20 Mbps in normal conditions. The 802.11g standard can scale back to support data rates of 48, 36, 24, 18, 12, and 9 Mbps.

Because 802.11g operates at the same frequency - 2.4 GHz - as 802.11b, devices are subject to the same limitations: only three non-overlapping channels and interference from unlicensed, non-protocol equipment. On the positive side, using the same 2.4 GHz frequency means that 802.11g devices are *backward-compatible* with 802.11b access points and other devices that enterprises may already have. However, different modulation techniques

prevent 802.11b and 802.11g devices from coordinating with one another to prevent collisions when using the same shared frequency. Thus the presence of an 802.11b station within range of an 802.11g access point forces the access point to invoke an RTS/CTS (Request to Send/Clear to Send) or CTS-to-self *protection mechanism*. This protected mode prevents simultaneous transmission by devices using 802.11g and 802.11b (which would result in collisions and retransmissions), but it significantly reduces the throughput of the overall wireless network. In protected mode, the access point drops down to 802.11b speeds to alert the 802.11b station that an 802.11g transmission is taking control of the media. To serve the 802.11b station, the access point must use DSSS modulation (rather than OFDM), and is thus limited to the lower data rates. Running in protected mode is required by standards whenever an 802.11b station is present.

IV. 802.11a

The IEEE 802.11a standard provides the same 54 Mbps maximum data rate as 802.11g. But unlike 802.11b and 802.11g, the 802.11a standard operates in the 5 GHz ISM band. This means that 802.11a devices are not subject to interference that affects 802.11g and 802.11b devices, but they are still subject to interference from other products designed to use this 5 GHz ISM band.

The 5 GHz band allocates up to 19 non-overlapping channels depending on local regulations. The higher data rate, coupled with more non-overlapping channels, enables greater density deployments (more access points within a given area) to accommodate more users and provide greater capacity.

With its high throughput and lower range, 802.11a is ideally suited for provisioning connectivity to densely populated user environments such as computer labs, classrooms, large conference rooms, airports or convention centers.

However, the 802.11a is subject to a basic rule of physics: the higher the radio frequency, the shorter the range. Because 802.11a operates in the 5 GHz band, its signal range is somewhat more limited than that of 802.11b/g, which operates at 2.4 GHz. The shorter wavelength radio signals have more difficulty penetrating walls and other obstructions. As a result, more access

points are typically required to cover a given area.

Without backward compatibility for the installed base of predominately 2.4 GHz-based wireless clients, 802.11a, by itself, never gained mass adoption in the business or home wireless networks. With the overall rapid industry growth of wireless and the technology advances that followed, today most mobile devices such as notebooks support both 802.11b/g and 802.11a. To follow suit, most access points also provide simultaneous 802.11b/g and 802.11a support.

V. 802.11n

The draft 802.11n standard defines a new physical layer for increasing the throughput of wireless local area networks. The 802.11 Task Group n (TGn), chartered by IEEE in January 2004, has spent more than two years drafting a new amendment to the 802.11 standard to address the need for higher throughput. The task group was presented with competing proposals by two large industry groups: the WWiSE (World-Wide Spectrum Efficiency) Alliance, backed by companies including Broadcom, and TGn Sync, which was backed by Intel and Philips. In 2005, WWiSE and TGn Sync, along with a third group called MITMOT, merged their respective proposals into a joint draft.

802.11n is based on MIMO (multiple input/multiple output) OFDM technology, which allows the transmission of up to 100 Mbps over a much wider range than earlier versions. MIMO uses multiple transmitters and receivers to allow for increased throughput through spatial multiplexing and increased range.

In January 2006, TGn voted unanimously to confirm selection of a joint proposal for high throughput WLANs. The 802.11n amended standard specifies methods of increasing the signaling speed of wireless LANs up to 600 Mbps – more than 40 times faster than 802.11b and near 10 times faster than 802.11a or 802.11g. It is projected that 802.11n will also offer a better operating distance than current networks.

At its March 2006 meeting, the TGn group sent the 802.11n draft for a comprehensive review by more than 500 technical experts from leading technology companies, academic institutions, and government agencies. The IEEE 802.11n standards

development project expects to complete its draft development work in late 2006, with final ratification and publication of the formal 802.11n amendment sometime in 2007.

As wireless and related technologies continue to mature, it is more apparent than ever that well-formed standards are the most intelligent way to ensure that future products meet the needs of the marketplace. The Wi-Fi Alliance and other industry groups have advocated strongly against the introduction of “pre-N” products, arguing that there is no way to guarantee these early entry products will be compatible with the eventual standard. The Gartner Group has urged enterprises to “plan to stay with Wi-Fi-certified products” (that is, 802.11a,b,g) and avoid adopting “premature” products based on a specification that is still in flux and likely to undergo changes before its final ratification.¹

VI. Implementation Considerations

Which type of wireless network: centrally coordinated or standalone AP?

Both the standalone and centrally coordinated architectures have advantages and disadvantages, depending on the age of the wired infrastructure, deployment area, building architecture, and types of applications that you want to support. Regardless which approach you choose, it is essential that your architecture provide you with a way to manage your network efficiently and effectively.

A *standalone access point* WLAN is particularly well suited in environments where:

There is a smaller isolated wireless coverage area that requires only one or a few access points.

There is a need for wireless bridging from a main site building to a branch office or to a remote portable or temporary building such as a portable classroom.

However, the operational overhead to manage and maintain a wireless LAN increases with the size of the wireless LAN deployment. Wireless LAN management tools like ProCurve Manager and Airwave Management Platform help simplify configuration and monitoring of the LAN, but the inherent “independence” of these access points presents a challenge in addressing

security, configuration control, bandwidth predictability, and reliability, as users and applications become dependent on an always available and reliable wireless LAN connection. A *centrally coordinated* WLAN is well suited to deployments where:

There are one or more large wireless coverage areas that require multiple radio ports possibly accompanied by several smaller isolated coverage areas.

RF network self-healing is required.

A redundant stateful-failover solution is required.

In a recent market analysis, IDC estimated that “dependent” access points - where most network management and other functions are dependent on a centralized controller such as the ProCurve 5300xl Wireless Edge Services Module - “will grow to represent 74% of all enterprise access point shipments in 2009.”² What’s more, as wireless LAN deployments continue to grow larger, accommodating ever greater numbers of users, there will be an increasing demand to centrally manage a wide range of security, performance and configuration attributes as a single system.

A centrally coordinated network offers many benefits, including:

Lower operational costs. Centralized management facilitates ease of deployment and ongoing management.

Greater availability. In this architecture, it’s easier to respond in real-time to changes in the network performance and spikes in user demand.

Better return on investment. Fast client roaming and enhancements in Quality of Service enable traffic-sensitive applications such as voice over wireless LAN.

Coordinated AP deployments are most appropriate in larger organizations with a wireless overlay throughout the facility, campus-wide. This kind of deployment allows a facility to address operational concerns, simplify network management, and assure availability and resiliency - with more users, it’s essential to minimize help desk calls and trouble tickets. There are many different ways to set up your wireless network. Of course, you’ll need a certain density of access points to provide

satisfactory network coverage and capacity. While many aspects of wireless LAN are analogous to wired LAN and should be managed in a consistent fashion, some aspects of wireless are unique. Wireless radio is a shared medium and, as such, requires careful planning for dynamic usage profiles and capacity variations.

VIII. Dual-band radios and dual radio access points

802.11a/b/g dual-band access points with two radios can simultaneously support both 2.4 GHz (802.11b/g) and 5 GHz (802.11a) RF bands. They offer backward compatibility (to preserve existing investments) along with a larger number of channels and consequently increased throughput. A wireless station with a dual-band radio

VII. The Pro Curve Solution

Through its active and extensive participation in standards bodies, ProCurve has demonstrated its leadership in the development of industry standards, spearheading much of the work that goes into their formation and adoption.

According to IDC, “a strong vendor-neutral interoperability and technology advocacy organization ... will continue to ensure a consistent user experience between products from multiple vendors.”³ Because ProCurve solutions are standards-based, they are interoperable with many authentication systems, clients, and switches. Companies can leverage existing site infrastructure investments without sacrificing security or functionality. The ability to reap the benefits of a secure WLAN without re-tooling the entire network infrastructure can provide huge cost savings.

Based on the ProCurve Networking Adaptive EDGE Architecture™, ProCurve networking solutions not only include hardware and software, but also the services, support, and tools necessary to enable a successful, cost-effective WLAN deployment regardless of the existing infrastructure. With a lifetime warranty and free software updates, ProCurve Networking products provide investment protection to the customer.

The ProCurve Networking Adaptive EDGE Architecture provides unified security and unified management capabilities across the

typically looks first for an 802.11a access point. If it cannot find one, it then scans for an 802.11g, and ultimately for an 802.11b.

Dual-band access points are well suited to a wide range of network topologies. In addition to the benefits of increased bandwidth, it is fairly common to find deployments that use dual-band access points to segregate data types onto the different RF bands. The access point's 802.11a radio can service wireless traffic from data clients (such as notebooks), while the 802.11b/g radio supports time-sensitive voice traffic from VoWLAN handsets, thus reducing data and voice traffic contention by creating two separate RF networks.

entire wired and wireless infrastructure, enabling network administrators to easily deploy and centrally manage a secure, yet flexible, multi-service network.

Complementary products and technologies

ProCurve understands the importance of centralized management of the network and provides a comprehensive set of network management tools to support both centralized and standalone AP network architectures.

For distributed sites such as remote or branch offices, ProCurve offers the Access Point 530, a secure, dual-radio highly intelligent standalone access point that provides a comprehensive range of industry-proven security capabilities that integrate easily into any network design. In addition to supporting dual radio (802.11b/g + 802.11a) operation to service dual-band wireless clients, the Access Point 530 can be configured as a dual 2.4GHz (802.11b/g + 802.11b/g) access point to provide high capacity data and voice coverage in networks where support for 802.11a is not a requirement.

To accommodate a wide range of mainstream deployments, the access point includes both 2.4 GHz and 5 GHz integrated diversity omnidirectional antennas for easy deployment as well as external antenna connectors compatible with ProCurve's line of external antennas to extend wireless coverage or wireless bridging to remote

access points. ProCurve offers a variety of antennas that customers can choose to address needs that were identified during the site survey.

The ProCurve Access Point 530 provides a built-in RADIUS authentication server that enables enterprise 802.11i wireless security. This provides enhanced security (such as dynamic encryption keys and periodic key rotation) for deployments that cannot utilize a remote RADIUS server.

ProCurve intelligent edge switch 5300xl series offers identity driven access control to network resources over wired network connections. Now with the addition of the ProCurve Wireless Edge Services xl Module, these same role-based access policies, dynamically generated by ProCurve Identity Driven Manager, are now enforced across the wireless edge. This unified approach to wired and wireless policy management provides edge-enforced security and network access control on every network connection regardless if a user connects to the network via wireless or through a wired port. The Wireless Edge Services Module provides centralized RF configuration and control over a group of 210/220/230 Radio Ports and their corresponding wireless coverage area(s).

Working in conjunction with ProCurve Radio Ports, the Wireless Edge Services Module enables advanced services such as RF network self-healing, fast roaming, and QoS prioritization to assure that the wireless LAN remains resilient and reliable. As the wireless network expands, it's easy to increase the radio port capacity by purchasing additional software licenses. Both the ProCurve Access Point 530 and the ProCurve Wireless Edge Services xl Module include built-in support for ProCurve Manager Plus (PCM+), including ProCurve Mobility Manager and ProCurve Identity Driven Manager (IDM). Network administrators can easily manage their entire unified network, including wired and wireless devices, as well as administer security and role-based user policies that are enforced regardless of how or where the user connects to the network.

By providing centralized control of wired and wireless access and security policies, and centralized management of the wired and WLAN infrastructure, PCM+ also decreases operational costs and increases the productivity of information technology (IT) personnel. With simplified system management capabilities, PCM+ offers centralized visibility, configuration and modification for a widespread WLAN

deployment.

IX. References:

1. Address Allocation for Private Internets
 - RFC 1918 BGP, Border Gateway Protocol
 - RFC 1771 RIP, Routing Internet Protocol
 - Version 1, RFC 1058
 - Version 2, RFC 2453
2. OSPF, Open Shortest Path First
 - 21 Wireless Network Structure - v1.3*
 - Version 2, RFC 2328
 - Version 3, RFC 2740 (for IPv6)
3. DHCP, Dynamic Host Control Protocol
 - RFC 2131
 - R. Droms, "Dynamic Host Configuration Protocol", 3/97. <http://www.dhcp.org>
 - <http://www.dhcp.org> Zebra, A routing software package for TCP/IP networks
 - <http://www.zebra.org> (<http://www.zebra.org>) Wireless Router HOWTO
 - <http://www.rage.net/wireless/wireless-howto.html>
 - <http://www.rage.net/wireless/wireless-howto.html>) Building Wireless Community Networks
 - O'Reilly and Associates, January 2002
 - Rob Flickenger
 - ISBN 0-596-00204-1
4. Designing Large-Scale LANs
 - O'Reilly and Associates, January 2002
 - Kevin Dooley
 - ISBN 0-596-00150-9 802.11b protocol
 - <http://standards.ieee.org/getieee802/portfolio.html?agree=ACCEPT> (<http://standards.ieee.org/getieee802/portfolio.html?agree=ACCEPT>) Melbourne: Digital and Wireless networking RFC
 - <http://www.wireless.org.au/wiki/?RFC> (<http://www.wireless.org.au/wiki/?RFC>) Melbourne: Digital and Wireless Architecture 22
 - <http://www.wireless.org.au/wiki/?architecture> (<http://www.wireless.org.au/wiki/?architecture>)
 - Reliable Internet Connectivity with BGP <http://www.bgpbook.com/> (<http://www.bgpbook.com/>)