Independent Consulting Services

Wireless Network Industry Report

2007

For an update on the wireless industry,
please contact us at info@wireless-nets.com

Author: Jim Geier
Principal Consultant, Wireless-Nets, Ltd.
Email: jimgeier@wireless-nets.com
Website: www.wireless-nets.com

About the Author

Jim Geier is the founder of Wireless-Nets, Ltd. and the company's principal consultant. His 25 years of experience includes the analysis, design, software development, implementation, installation, and support of numerous wireless network-based solutions for municipalities, enterprises, airports, homes, retail stores, manufacturing facilities, warehouses, hospitals, and product manufacturers worldwide. Jim is the author of over a dozen books, including Implementing 802.1X Security Solutions (Wiley), Deploying Voice over Wireless LANs (Cisco Press), Wireless LANs (SAMS), Wireless Networking Handbook (Macmillan), and Network Reengineering (McGraw-Hill). He is the author of numerous tutorials for www.Wi-FiPlanet.com and other publications and has developed and instructed dozens of training courses on wireless networking topics. Jim has been active within the Wi-Fi Alliance, responsible for certifying interoperability of 802.11 (Wi-Fi) wireless LANs. He has also been an active member of the IEEE 802.11 Working Group, responsible for developing international standards for wireless LANs. He served as Chairman of the IEEE Computer Society, Dayton Section, and Chairman of the IEEE International Conference on Wireless LAN Implementation. He is an advisory board member of several leading wireless LAN companies. Jim's education includes a bachelor's and master's degree in electrical engineering and a master's degree in business administration.

Contact Jim Geier at jimgeier@wireless-nets.com

Wireless Nets, Ltd.

Wireless-Nets, Ltd. provides independent technical and business consulting services, assisting firms with the development of wireless products and deployment of wireless networks into corporate information systems. Services include the following:

- System Deployment - Services that assist IT organizations and system integrators with the design, installation, testing and operational support preparations of wireless networks.
- Product Development - Services that assist product developers with the integration of wireless network interfaces into their products.
- Training - Services that prepare IT organizations, system integrators, and product developers with the development and deployment of wireless network solutions.

Contact Wireless-Nets, Ltd. at info@wireless-nets.com

Table of Contents

1. Wireless PAN Solutions

This section of the report discusses the various wireless PAN technologies.

1.1 Bluetooth

Bluetooth is a specification published by the Bluetooth Special Interest Group (SIG), with big promoters including 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia, and Toshiba. This specification offers secure, low power, short-range transmissions of data and voice at up to 3Mbps in the 2.4 GHz frequency band.

1.1.1 General Attributes

Bluetooth includes the following general attributes:

- Medium performance

  Bluetooth provides up to 1 Mbps for Version 1.2 of the Bluetooth specification and up to 3 Mbps supported for Version 2.0 + EDR (Enhanced Data Rate) Bluetooth specification. EDR performance is currently not good enough for applications beyond simple cable replacements for data and voice. The higher data rate of 802.11 offers significant competition.

- Short to medium range

  Class 3 radios offer approximately 3 feet range. Products based on these type radios are uncommon. Class 2 radios are the most commonly found in mobile devices and provides approximately 30 feet range. This range makes Bluetooth suitable for simple cable (USB and serial) replacements with requirements for relatively low data rates. Class 1 radios are used primarily in industrial use cases and provide up to 300 feet range. There are not many of these devices available. Deployments are rare and compete heavily with 802.11/Wi-Fi. As a result, Bluetooth wireless LANs will likely not proliferate.

- Low power

  Class 2 devices operate at 2.5 mW. This makes Bluetooth ideal for small client devices, such as mobile phones and bar code scanners.

- Low cost

  Bluetooth is suitable for lower-cost client devices having limited margins.

1.1.2 Technology and Issues

Bluetooth operates in the 2.4GHz band using frequency hopping spread spectrum (FHSS), which includes 79 channels and a very high hopping rate. FHSS spreads the signal power across the entire 2.4GHz band. As a result, Bluetooth offers potential outward interference with 2.4GHz 802.11/Wi-Fi networks. It's not possible to tune 2.4GHz 802.11/Wi-Fi access points to channels that avoid the FHSS interference. This has caused significant concern among enterprise IT managers, but the relatively low power of Bluetooth keeps actual interference to manageable degrees.

The IEEE 802.15.1 standard is based on the initial Bluetooth specification. IEEE 802.15.3 is a draft standard currently under development that is targeted data rates of 20 Mbps. This will address higher performance needs for simple cable replacement applications, but it will not likely compete with 802.11/Wi-Fi due to likely proliferation of 802.11n.

IEEE 802.15 Task Group 5 is developing a mesh version of the standard. This could enable a wider coverage area without the need for access points for some applications, which could reduce costs for widespread deployment and enable new applications (e.g., ad hoc networking).

1.1.3 Applications

Bluetooth is designed to satisfy requirements for personal area networking, not LANs. This makes Bluetooth most suitable for primarily USB and serial cable replacement for printers, mobile phones, headsets, and laptops. As these products have been made available, consumer reviews have been very good. Consumers find them simple to use and offer tremendous value.

1.1.4 Vendors / Products

The Bluetooth Special Interest Group (SIG) has a program to ensure compliance with Bluetooth specifications. Based on the official Bluetooth website, there are many qualified Bluetooth product (refer to https://programs.bluetooth.org/tpg/listings.cfm). Bluetooth radio modules are well developed, tested, and included in many different consumer products. This provides a stable development platform for continuing the integration of Bluetooth into products.

1.1.5 Proliferation and Future Outlook

Bluetooth is by far the leading wireless PAN solution. The majority of mobile phones and other mobile devices implement Bluetooth, and mobile device consumers are

commonly familiar with Bluetooth applications. With the mass of vendors offering Bluetooth products and solutions, Bluetooth will likely remain the primary wireless PAN solution for the foreseeable future. In general, strong activity in standards group, such as Bluetooth, also provides a good basis for proliferation.

1.2 Zigbee

The Zigbee Alliance, backed by members such as Siemens, Philips, Texas Instruments and Samsung, promotes a wireless specification that offers low power and short to medium range transmission of data at up to 250Kbps in the 2.4GHz frequency band.

1.2.1 General Attributes

Zigbee includes the following general attributes:

- Low performance

  Zigbee focuses on providing relatively low data rates:
  - 250 Kbps at 2.4GHz
  - 40 Kbps at 915MHz
  - 20 Kbps at 868MHz

- Short to medium range

  Zigbee products have a range of 30 to 300 feet range, depending on the construction of the facility and operating frequency.

- Low power

  Zigbee radios have very low power consumption. As a result, the battery life is from months to years depending on radio duty cycle. This leads to new wireless applications, such as large density of electronic signs in a retail environment.

- Low cost

  Zigbee is more cost-effective than Bluetooth for low performance applications.

1.2.2 Technology and Issues

Zigbee is based on the IEEE 802.15.4-2006 and 802.15.4-2003 standards, which specify the use of direct sequence spread spectrum operating in several un-licensed bands: 868MHz, 915MHz and 2.4GHz. The ZigBee Alliance has a similar relationship with 802.15 as the WiFi Alliance has with 802.11, that is, the Zigbee Alliance provides

interoperability assurance and marketing functions. This allows member companies to better promote the technology.

The high utilization of nearby 802.11/Wi-Fi networks could cause significant inward interference to Zigbee solutions, but this will likely have very little impact on low duty cycle applications. For example, a telemetry application that transmits temperature information every minute will experience insignificant delays in the presence of interference.

1.2.3 Applications

Bluetooth can satisfy all wireless PAN applications, but Zigbee offers a lower cost and lower power alternative for lower performance applications. ZigBee technology is targeting the control applications industry, which does not require high data rates, but must have low power, low cost and ease of use (remote controls, home automation, etc.). Zigbee is an excellent technology for supporting limited wireless updates to many client devices. For example, Zigbee could effectively support the transmission of daily price updates to hundreds of electronic signs throughout a department store. The use of Bluetooth for even Wi-Fi for this application would be too costly and require frequent charging of the batteries in the electronic signs. Companies should consider using Zigbee as an alternative to Bluetooth for applications requiring low performance and long battery life.

1.2.4 Vendors / Products

There are very few certified Zigbee products to-date. Refer to the following URL for list of currently certified products:
http://www.zigbee.org/en/certification/certified_products.asp.
Promoter companies of the ZigBee Alliance include Philips, Honeywell, Mitsubishi Electric, Motorola, Samsung, BM Group, Chipcon, Freescale and Ember. There are approximately 70 other members. In relation to the Bluetooth SIG, Zigbee has very little participation. This is likely due to the somewhat limited scope of Zigbee applications. Zigbee offers significant value, but for a niche market.

1.2.5 Proliferation and Future Outlook

There are very few Zigbee deployments today. The low cost and extremely long battery life, however, will likely make Zigbee the leader in the niche market of low duty cycle / low power applications. Total proliferation will likely be significantly less than Bluetooth because of limited target applications.

1.3 Certified Wireless USB

The USB Implementers Forum (USB-IF) is a non-profit corporation founded by the group of companies that developed the Universal Serial Bus (USB) specification. The USB-IF has defined the Wireless USB specification, which targets 480Mbps at 3 meters and 110Mbps at 10 meters. Wireless USB utilizes the WiMedia MB-OFDM Ultra-wideband (UWB) radio platform as developed by the WiMedia Alliance. UWB operates from 3GHz to 10GHz, which is over the top of spectrum in use by other technologies and products. The UWB technology makes this possible, and it's approved by regulatory bodies, such as the FCC in the U.S.

The intent of Wireless USB is to provide an alternative to using USB cables. Cable has much more capacity than wireless transmission. As a result, Wireless USB will likely not totally replace USB cables because transfer speeds among peripherals, such as external hard drives, will likely continue to increase and exceed the capability of wireless technologies (but still be satisfied by cables).

Some vendors, such as Belkin, have begun selling Wireless USB devices. Others will likely follow, but so far vendors seem to be focuses on consumer-based USB cable replacement.

For a current update on Wireless USB, refer to the following website:
http://www.usb.org/developers/wusb/

2. Wireless LAN Solutions

There are a variety of technologies available for supporting wireless data communications within local areas, which primarily involves 802.11 / Wi-Fi standards.

2.1 Wi-Fi

Wi-Fi is the primary wireless LAN standard worldwide. Wi-Fi offers relatively high performance for general mobile, portable stationary applications.

2.1.1 General Attributes

Wi-Fi includes the following general attributes:

- High performance

  Wi-Fi currently offers up to 54 Mbps data rates using the IEEE 802.11a and 802.11g. 802.11n, which is currently emerging, is offering data rates at up to hundreds of Mbps. Some vendors implement faster rates based on proprietary features, but this requires the same vendor for the client radio and access point. This single vendor requirement can limit interoperability with some applications.

- Medium range

  The range of Wi-Fi with omni-directional antennas is highly dependent on facility construction and performance requirements. The typical effective range of an access point is 100 feet. The coverage general extends the size of a building with multiple access points. It's difficult to achieve 100 percent coverage in some environments, such as hospitals and warehouses. This leads to application problems and generally results in needs for wireless middleware to accommodate for erratic connectivity.

- Medium power

  Wi-Fi has moderate power requirements. Battery charge life is typically 20 percent less with an 802.11 radio operating. This is especially an issue for client devices not originally designed to operate with 802.11 radios, such as converting a batch data collector to a wireless device. 802.11 power-save features can improve battery life for lower duty cycle applications, but the actual battery life savings depends on access point settings and use of multicast traffic. The use of 802.11 power-save functions can also reduce application performance.

- Medium Cost

  It is moderately expensive to integrate Wi-Fi into client devices, as compared to Bluetooth. The higher cost, however, is reasonable in most cases, however, due to the much higher performance of Wi-Fi.

2.1.2 Technologies

Wi-Fi is currently based on the following standards:

- IEEE 802.11a

  The IEEE 802.11a standard specifies operation in the 5 GHz band at up to 54 Mbps data rates. As with all 802.11 systems, the data rate will automatically shift down to lower data rates to compensate for high retransmission rates. Actual throughput of 802.11 systems is approximately half of the associated data rate.

  802.11a is currently the optimum 802.11 technology in terms of capacity because of many non-overlapping channels and very low noise in the 5 GHz band. Range of 802.11a systems is not as limited as some tout. Higher transmit power and lower noise floor even provide better range than 2.4GHz systems in some cases. There is minimal RF interference due to many RF channels and noise floor that is generally very low (less than -90dBm) in most indoor and ground-level areas.

  There is limited deployment of 802.11a systems due to delays in product development as compared to 802.11b/g. There is currently less than 1 percent of 802.11 networks that implement 802.11a (based on extensive scans Wireless-Nets has completed in major cities). 802.11a will likely not be widely adopted because of the pending proliferation of the higher performing 802.11n solutions. 802.11a, however, could fulfill niche markets due to relatively low power requirements.

- IEEE 802.11g

  The IEEE 802.11g standard offers data rates of up to 54 Mbps in the 2.4 GHz band. 802.11g access points are backward compatible with older 802.11b client cards. 802.11g is currently the most commonly and widely distributed wireless LAN standard. Even though 802.11g offers the same data rates as 802.11a, 802.11g has less capacity because of the use of only three non-overlapping RF channels.
  802.11b and 802.11g systems both encounter significant RF interference from microwave ovens and cordless phones as described in the following section.

  Many 802.11g implementations use 802.11b-only mode to avoid issues interoperability issues and maximize range. Sometimes 802.11b client radios

have trouble connecting to 802.11g access points, and administrators often fix the problem by switching the 802.11g access points to b-only mode. 802.11b also has slightly better range due to lower minimum data rate. 802.11b can operate with data rates as low as 1 Mbps; whereas, 802.11g can only operate as low as 6 Mbps. The lower minimum data rate operation of 802.11b allows longer range operation as compared to 802.11g. In addition, most 802.11g access points set to b-only mode will send beacons as 1 Mbps instead of 2 Mbps (which is what 802.11g uses). This extends the reach of 802.11b access points beyond 802.11g access points. In addition, the use of b-only mode eliminates the need for the access point to use protection mechanisms since users are all 802.11b and not a mix of 802.11b and 802.11g.

- IEEE 802.11n

  IEEE will be ratifying the IEEE 802.11n standard, with data rates of a couple hundred Mbps, within the next year or so. Pre-802.11n standard products have been available for the past year, and Cisco recently announced the availability of their enterprise 802.11n solution. 802.11n makes use of both 2.4GHz and 5GHz bands, makes use of MIMO technology, and is backward compatible with 802.11a/b/g. It's likely that 802.11n will proliferate heavily throughout homes and enterprises as the leading wireless LAN standard, mostly replacing 802.11a/b/g within the next few years. 802.11n should start appearing in handheld devices, such a PDAs, when 802.11n starts showing definite signs of proliferating in hotspots and enterprises, which will be approximately 2009. As a result, companies should consider the integration of 802.11n into products.

2.1.3 Deployment Issues

The following discusses some of the primary issues with deploying Wi-Fi networks:

- Spotty Signal Coverage

  Most Wi-Fi installations have spotty signal coverage. This introduces risks for deploying mobile applications over existing Wi-Fi networks. A common mistake made during installation is to neglect weaker uplink signal strengths, which emanate from the client radio card (e.g., integrated in a bar code scanner or laptop). Instead, installers measure the downlink signal strength to determine whether or signal coverage exists. The downlink signal strength is much higher than the uplink, which leads to erroneous signal coverage measurements. The downlink signals may be strong enough, but the uplink signals fall short of maintaining connections within the expected signal coverage. In order to deploy an optimum network, it's important to take into account weaker uplink signals when designing and verifying Wi-Fi networks.

- Limited Voice Capacity

  802.11g and 802.11b systems have less capacity for simultaneous voice users than what would be expected, mainly because voice packets are relatively small (couple hundred bytes each), which requires a significant amount of overhead. Cisco has determined that an 802.11b access point, for example, can support up to 15 simultaneous voice users[1]. In order to allow sufficient bandwidth (40 percent) for data as well, an 802.11b access point is limited to 8 simultaneous calls. This assumes that the users are obtaining 11 Mbps connections, which is not common throughout typically installed wireless LANs. Generally, the associated data rates are less, such as 2 Mbps. 802.11g access points can support a greater number of simultaneous voice calls, but this is somewhat limited by the use of protection mechanisms in a mixed 802.11b and 802.11g user environment. 802.11n will help significantly increase the number of supported simultaneous voice users. If there's a need to maximize the number of supported simultaneous voice users, then consider deploying 802.11a or 802.11n wireless LANs.

- Denial of Service (DoS)

  A denial of service (DoS) attack is an assault that can cripple or disable a wireless LAN. Wireless networks are extremely vulnerable to DoS attacks, which can cause a wireless LAN to slow to crawling speeds or actually quit working. This causes a company that's dependent on a wireless LAN to experience delays, which can be costly for some applications such as wireless security cameras, inventory systems, and point of sale terminals.

  One form of DoS attack is the "brute force" method. This type of attack can come in one of two forms: either a huge flood of packets that uses up all of the network's resources and forces it to shut down, or a very strong radio signal that totally dominates the airwaves and renders access points and radio cards useless.

  One of the ways a hacker can perform a packet-based brute force DoS attack is to use other computers on the network to send large numbers of useless packets to the server. This adds significant overhead on the network and takes away useable bandwidth from legitimate users.

  The use of very strong radio signal to disrupt the access points and radio cards is a rather risky attack for a hacker to attempt. Because a very powerful transmitter at a relatively close range must be used to execute this type of attack, the owners of the wireless LAN can find the hacker through the use of homing tools, such as AirMagnet.

[1] Source: "Cisco Wireless IP Phone 7920 Design and Deployment Guide" (refer to the section titled "Throughput Calculations for 802.11b WLAN").

Sometimes a DoS occurrence on a wireless network may not even be intentional. Because 802.11b/g resides in such a crowded spectrum; 2.4GHz cordless phones, microwaves, Bluetooth, and other devices that use the 2.4GHz spectrum may cause a significant reduction in 802.11b performance.

A company can protect a wireless LAN against DoS attacks by making the building as resistive as possible to incoming radio signals. The following are some steps to help minimize radio signals from getting inside the building:

- Paint exterior walls with special “attenuation paint.”
- If interior walls are using metal studs, make sure they are grounded.
- Install thermally insulated copper or metallic film-based windows.
- Use metallic window tint instead of blinds or curtains.
- Use metallic-based paint on the interior parts or the exterior walls.
- Aim directive access point antennas towards the inside of the building.

The problem with these solutions, however, is that they can be expensive and also cuts off the usage of other wireless devices, such as cell phones. It also is not effective if a hacker some how gets “inside the cage.”

Something that should be put in place for any wireless LAN application that is mission critical is a backup plan. A company should not be so dependent on their wireless network that if it goes down, everything grinds to a halt. A company should have a “plan B” in case the wireless LAN becomes unavailable due to a DoS attack. In addition, special consideration should be given to installing a wireless LAN where life or considerable finances are at stake in the event that the wireless LAN becomes inoperable.

- RF Interference

RF interference causes wireless clients and access points to hold off transmitting, which causes delay and lower throughput. This resulting decrease in performance can make browsing websites and downloading files sluggish and severely limit the number of active voice users. In cases where interfering signals are strong enough, the wireless clients may not be able to access the wireless LAN at all for an indefinite period of time. This is rare, but possible. As a result, companies need to be aware of potential source sources of RF interference, such as microwave ovens and cordless phones, which are operating within the wireless LAN environment.

For example, Wireless-Nets recently completed testing to understand how much impact a typical microwave oven has on wireless LAN operation. We did the testing within a typical small office area. A single 802.11b access point covers the entire facility. The microwave included in the testing is made by GoldStar and resides in a break room. The label on the back of the microwave indicates that it

consumes 1,200 watts of power and operates at 2,450 MHz, which is close to 802.11b/g channel 9.

Before turning on the microwave, we set the access point to channel 9 (a worst case situation), and took some measurements within the break room to use as a baseline. The access point signal level resulting from the beacons within the break room was -63dBm, sufficient for solid 11Mbps associations. Throughput tests indicated 667 packets per second (pps) while sending 1,532 byte frames. While holding the wireless client (a laptop) within one foot of the microwave, we recorded some measurements while the microwave was set to high and heating up a large bowel of water. The throughput fell to 90pps, a significant drop. As a result, using a wireless client very close to the operating microwave made the throughput plunge by over 85 percent. This is a substantial reduction in performance, but it's the worst case situation. The access point was set to the same frequency of the microwave, and it's unlikely that someone would use a wireless client so close to the microwave.

A more realistic distance from the microwave is from one of the break tables, which is about eight feet away from the microwave. At this range, we reran the throughput tests, resulting in 178pps. This still equates to around a 75 percent decrease, which is still substantial. In order to experience a 75 percent decrease in throughput, we tried surfing to a web site having a few graphics. With the microwave running, the pictures would come in painfully slow. We also surfed around a bit to other pages, and sometimes the pages would freeze. After turning off the microwave, we cleared the browser cache and found no problems surfing the same web pages.

We also repeated the tests down the hall about twenty feet away with the microwave running and still experienced fairly sluggish responses. In fact, throughput from there was still only 260pps. Obviously, the microwave was making the wireless LAN very slow at surprisingly great distances from the microwave. Something to consider is that these tests were run with only one active wireless client. The results would have been much worse if there were more users on the network.

Curious to know what channels the microwave would affect the most, we reran the throughput tests again while the access point was set to different channels. With the access point set to channels 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11, the throughput was 660pps, 658pps, 655pps, 651pps, 643pps, 574pps, 434pps, 258pps, 178pps, 191pps, and 210pps, respectively. Based on these numbers, the microwave was most critically impacting channels 8, 9, 10, and 11.

After researching typical consumer and commercial microwave ovens, we've found that most microwave ovens also offer significant RF interference in the upper one-third of the 2.4 GHz band, similar to the Goldstar microwave oven. As

a result, consider avoiding the upper third of the 2.4 GHz band when installing 802.11b/g access points in areas where there are microwave ovens.

2.4 GHz cordless phones have also been known to cause interference to wireless LANs. Today, a person can purchase cordless phones that operate in a variety of unlicensed frequency bands: 900 MHz, 2.4 GHz, and 5 GHz. The phones causing the greatest potential for interfering with wireless LANs, especially 802.11b and 802.11g, are ones based on 2.4 GHz. Many of these phones utilize direct sequence spread spectrum and automatically choose the least congested channel. If only installing one or two access points set to non-overlapping channels, there is enough room left in the 2.4 GHz band for the phone to tune to without causing interference to the Wi-Fi network. For larger Wi-Fi networks, where all three non-overlapping channels are utilized in most areas of the facility, cordless phones can cause a significant level of RF interference. If possible, the use of 2.4G GHz cordless phones should be prohibited in cases where it's critical to maximize the capacity of a Wi-Fi network, such as the case when maximizing the number of active voice users.

2.1.4 Architectures

The following discusses various architectural considerations for Wi-Fi networks:

- Thick Access Points

  Most access points, especially those for enterprises, traditionally have intelligence beyond what the 802.11 standard provides. These access points are often referred to as "thick" or "intelligent" access points. An enterprise grade thick access point will implement advanced functions that enhance security, management, and performance. In some cases, a thick access point will even implement higher layer functions, such as dynamic host configuration protocol (DHCP) and network address translation (NAT). Thick access points connect to conventional Ethernet switches, which provide a wireless LAN backbone infrastructure in an enterprise. The switches in this case don't usually have any features that enhance wireless communications.

  These traditional enterprise grade access points are relatively expensive as compared to the "thin" access points discussed later in this report. As a result, it's costly to scale up the wireless LAN based on thick access points when installing additional access points to increase coverage or performance. In addition, the "thick" access point approach is costly to migrate to newer technologies. In some cases, a company can merely upgrade the firmware of the access point to begin implementing modifications, such as WPA. The deployment of some technologies, such as AES, will likely require replacing the access points. Consequently, the "thick" access points can be expensive to support. Also in regards to support, "thick" access points have lots of configuration parameters that operational support software must interface with. This places a significant

amount of over head traffic over the network, which can decrease available throughput for primary applications.

- Thin Access Points

  The trend today for enterprises is to deploy “thin” access points that minimize the intelligence in the access points and employ a central wireless switch. This centralizes the intelligence in the switch instead of the access points. With this approach, the relatively simple access points can share the features that enhance wireless communications in a cost-effective and efficient manner. Because the “thin” access points don’t implement much more aside from the 802.11 standard, they are generally less costly. This can reduce the total cost of ownership of a wireless LAN because of less expensive upgrades and migration to future technologies.

  Much of the configuration is centralized in the wireless switch, which reduces management functions from operating over the wireless LAN. An administrator can interface directly with the switch from the more familiar wired side of the network. The central nature of the switch makes it an excellent platform for managing the network. In addition, the wireless switch optimizes performance. Roaming handoffs are much faster than conventional switches, which makes it more practical to effectively support voice over wireless solutions.

  The Control And Provisioning of Wireless Access Points (CAPWAP) specification enables the development of thin access points from multiple vendors that interoperate with an access controller. Light Weight Access Point Protocol (LWAPP) had been proposed by authors from Airespace, DoCoMo and Legra and several vendors were starting to implement it. Rather than adopt LWAPP, however, IETF formed a Working Group to look at the overall management of access points with representations from Trapeze, Airespace, and Chantry. The CAPWAP specification is needed to keep the wireless LAN industry from splintering the backend. The existing thin access point solutions utilize proprietary versions of LWAPP, but CAPWAP will eventually drive prices down if approved and implemented. Refer to the following websites for more information on CAPWAP:

  - http://tools.ietf.org/wg/capwap/
  - http://www.ietf.org/html.charters/capwap-charter.html

  When deploying a wireless LAN, strongly consider the use of “thin” access point solution that makes use of a wireless switch that enhances operation of the wireless LAN.

- Multiple SSIDs

  A service set identifier (SSID) is a unique label that distinguishes one wireless LAN from another. Wireless devices use the SSID to establish and maintain connectivity. As part of the association process, all radio cards must have the same SSID as the access point. An SSID contains up to 32 alphanumeric characters, which are case sensitive. Traditional access points are only capable of supporting a singe SSID.

  Some vendors, such as Cisco and Motorola/Symbol, are offering access points that support multiple SSIDs. This logically divides the access point into several virtual access points all within a single hardware platform. Many companies want to take advantage of this technology because using access points to support more than one application, such as public Internet access and inventory control, increases flexibility and keeps costs down.

  Multiple SSIDs allow users to access different networks through a single access point. Some examples of products that support multiple SSIDs are the Cisco 1100 Series access point, which can support up to 16 separate SSIDs, and the Symbol Mobius Axon Wireless Switch, which can support up to 32 separate SSIDs. Network managers can assign different policies and functions for each SSID, increasing the flexibility and efficiency of the network infrastructure.

  The following are settings that can apply to each SSID:

  - Virtual Local Area Network (VLAN). If the network uses VLANs, it's possible to assign an SSID to VLAN1, and the access point groups client devices using that SSID into VLAN1. This enables the separation of wireless applications based on security and performance requirements. For example, one could enable encryption and authentication on a particular SSID to protect private applications and no security on another SSID to maximize open connectivity for public usage.
  - SSID broadcasting. In some cases, such as public Internet access applications, it's advantageous to broadcast the SSID to enable user radio cards to automatically find available access points. For private applications, it's generally best to not broadcast the SSID for security benefits. Multiple SSIDs on a single access point let you mix and match the broadcasting of SSIDs.
  - Maximum number of client associations. It's possible to set the number of users that can associate via a particular SSID, which makes it possible to control usage of particular applications. This can help provide a somewhat limited form of bandwidth control for particular applications.

  The use of multiple SSIDs enables more flexibility when deploying a shared wireless LAN infrastructure. Instead of supporting only one type of application, possibly one that requires significant authentication and encryption, the wireless

LAN can also maintain other applications that don't require such stringent controls. For example, the access point could support both public and operational users from a single access point.

The benefits of a shared infrastructure are certainly cost savings and enabling of mobile applications. Rather than having two separate wireless LANs (which probably isn't feasible), a company can deploy one wireless LAN and satisfy all requirements. The combination of multiple applications enables the ones having lower return on investment to be part of the wireless LAN. Sometimes a company needs to have several applications supported together to make the costs of deploying a wireless LAN feasible. As a result, consider integrating applications with multiple SSIDs if there are benefits for configuring wireless settings different for each application.

2.1.5 Applications

Wi-Fi-based wireless LANs have applications in many in-building environments, such as homes, offices, warehouses, schools, hospitals, and airports. The performance of current 802.11g and future 802.11n networks are comparable to wired Ethernet networks, making them feasible for supporting a wide variety of mobile applications. The applications are endless.

Wireless IP telephony applications are continuing to proliferate over Wi-Fi networks as more and more enterprises install higher-performance wireless LANs based on 802.11g and 802.11n technologies. A warehouse, for example, will equip clerks with Wi-Fi phones to avoid using problematic two-way radios and improve communications. Many facilities, such as hospitals, don't have sufficient cell phone coverage and strongly benefit by making use of Wi-Fi phones for doctors and nurses rather than pay relatively high fees for extending cell phone coverage indoors.

2.1.6 Vendors / Products

Cisco is by far the leading enterprise Wi-Fi vendor. Cisco has the Cisco Compatible Extensions (CCX) Program that provides guidelines for Wi-Fi vendors to manufacture Wi-Fi products that implement Cisco proprietary features, such as Cisco LEAP. Many of the larger organizations have exclusive contracts with Cisco for providing Cisco wireless LANs. Some of the startups, such as Aruba, are offering innovative wireless LAN solutions, with enhancements that go beyond the 802.11 / Wi-Fi standards. Motorola/Symbol offers a wireless LAN solution that has been dominating the retail environment for years. Motorola/Symbol is currently suing Aruba for patent infringement of Symbol's wireless LAN technology. The outcome of this lawsuit is not known yet, but it could weaken Aruba's stance in the market.

Wi-Fi products are very mature due to stable and evolving standards and significant proliferation of products in both consumer and enterprise markets. There are many Wi-Fi certified products. Refer to the following website for a list of currently certified Wi-Fi products: http://certifications.wi-fi.org/wbcs_certified_products.php?lang=en. Most of these vendors differentiate themselves by incorporating proprietary performance enhancements. This generally requires a common vendor for client radios and access points, however.

The following are current 802.11n chipset makers:

- Atheros
- Broadcom
- Marvell, Qualcomm
- Metalink
- Raylink

2.1.7 Proliferation and Future Outlook

Currently the most common Wi-Fi network that enterprises (and consumers) deploy is based on 802.11g. Based on comprehensive testing that Wireless-Nets has completed in major cities, such as San Francisco and Los Angeles, the deployment of Wi-Fi networks is widespread. For example, there is an estimated 40,000 Wi-Fi network within the City of San Francisco (50 square miles). Most consumers of laptops are very familiar with and want to take advantage of using Wi-Fi hotspots. This along with enterprise applications will continue to strengthen Wi-Fi's position in the market.

Some enterprises are deploying 802.11a in order to take advantage of the more stable operating environment in the 5 GHz band (due to less RF interference). Wireless-Nets has found that less than one percent of the wireless LANs in cities tested are 802.11a networks, however. Broadcom is implementing 802.11a technology with lower-power chipsets, which could lead some enterprises into deploying more 802.11a networks even as 802.11n proliferates. It's very likely that 802.11a will be a very small player, though, as 802.11n products proliferates.

2.2 802.11 FHSS

The initial 802.11 standard ratified in 1997 includes a physical layer that is based on frequency hopping spread spectrum (FHSS). FHSS delivers 1 Mbps and 2 Mbps data rates in the 2.4 GHz band. Not many of the vendors sell FHSS wireless LANs today because the hardware is rather costly, and almost everyone is deploying 802.11g. FHSS networks are still out there, however, in hospitals, warehouses, and manufacturing plants, supporting applications that have been around for a decade or so.

FHSS has not and likely will not be adopted as part of the Wi-Fi standard. As a result, FHSS systems will likely become obsolete. The HomeRF group tried to revive the use of FHSS for home networks, but that group failed to produce a viable standard that could compete with Wi-Fi and disbanded several years ago. As a result, you should not consider integrating products with 802.11 FHSS systems.

FHSS systems transmit data by hopping from one channel to a different channel (with a total of 79 channels in the U.S.) at least every 0.4 seconds according to a particular hopping sequence that uniformly distributes the signal across the entire 2.4 GHz frequency band. In comparison, 802.11b/g systems are set to a specific frequency, such as channel 6, and only transmit a signal that occupies roughly one third of the 2.4 GHz frequency band. A problem is that the 802.11 standard defines sets of specific hopping sequences that are designed to minimize interference among FHSS systems; however, the 802.11 FHSS standard offers no provisions for minimizing interference with 802.11b/g networks. This often results in significant RF interference that impacts 802.11b/g installations.

Because FHSS wireless LANs transmitting a frame spread there signal power over the entire 2.4-GHz band, FHSS hops all over the narrower 802.11b/g signals. No matter what channel is set in an 802.11b/g access point, the FHSS signal is always present. An 802.11b/g signal only interferes with roughly one third of the FHSS signal, however, which doesn't cause much damage. As a result, FHSS interferes much more with 802.11b/g rather than the opposite. Bluetooth and some 2.4GHz cordless phones also utilize FHSS, which can cause similar interference to 802.11b/g wireless LANs.

The following are tips to consider when a FHSS system is operating within the same vicinity as an 802.11b.g wireless LAN:

- When deploying a wireless LAN, always conduct a RF site survey, and analyze the presence of interfering RF sources. Understand that if FHSS networks are found operating in the local area, then you'll probably need to live with lower performance on an 802.11b/g network.
- Since FHSS spreads signal power over the entire 2.4GHz band, changing the 802.11b/g access point RF channel will not help. So, don't bother trying to find an optimum channel.
- If the resulting degradation of performance is acceptable, then there's probably no need to take any action. The presence of FHSS interference, however, could prompt you to install 5GHz (802.11a) wireless LANs, depending on the situation. The 5GHz band is relatively free from sources of RF interference, including FHSS systems.

Minimize deployment risks by carefully planning a wireless LAN deployment and make certain that issues, such as the presence of FHSS systems, are not going to be a problem.

3. Wireless MAN/WAN Solutions

The wireless MAN (metropolitan area network) and WAN (wide area network) industry has been growing significantly over the past few years to include higher performance connections using both licensed and unlicensed spectrum. The following sections describe the various types of wireless MAN/WAN technologies.

3.1 Wi-Fi Mesh

Wi-Fi mesh has evolved from traditional wireless LANs to include wireless connectivity and routing between access points. Many municipalities have either completed or are in the process of deploying Wi-Fi mesh systems. The use of Wi-Fi mesh solutions inside buildings and complex outdoor areas also offers advantages. A Wi-Fi mesh network includes mesh nodes distributed throughout an area. Each mesh nodes enables Wi-Fi connections with client devices, such as laptops, equipped with a Wi-Fi radio. Each mesh node communicates with each other wirelessly to form a mesh network that is capable of transporting data between users, servers, and connections to the Internet.

3.1.1 General Attributes

Wi-Fi mesh includes the following general attributes:

- Medium to high performance

  User access performance is based on Wi-Fi standard chosen, which is generally via 802.11b/g interfaces. 802.11a is seldom deployed. Most Wi-Fi mesh networks have bandwidth control, which is generally set (in city environments) to provide 1 Mbps uplink and downlink throughput per user.

- Medium range

  Signal coverage of a mesh network within a city environment is generally specified for 95 percent coverage outside and 70 percent indoors with use of indoor customer premise equipment (CPE). Generally, 30 t0 40 mesh nodes per square mile are necessary for full coverage outdoors. The actual number of nodes, however, depends on terrain and tree foliage. Wi-Fi mesh systems provide cost-effective signal coverage over small (e.g., 7 square miles of Miami Beach) and large metropolitan areas (e.g., 135 square miles of Philadelphia).

- Medium power

  End user devices have same power drain as standard Wi-Fi devices. Mesh nodes generally receive electrical power from mounting assets, such as light poles and traffic lights. This is sometimes an issue, especially with banked switched light poles. In general, mounting assets, such as light poles, are difficult to acquire because they are mostly owned by the electric companies. Solar panels are sometimes deployed to power some of the mesh nodes. This is relatively expensive initially but can lead to future cost savings through avoidance of paying for electricity.

- Medium to high cost

  Mesh node costs vary widely. Meraki sells outdoor mesh nodes for $100 each but provides limited configuration options. Meraki equipment, though, can satisfy a large number of applications. Consider using the lower cost Meraki devices for mesh network installations. The mainstream vendors, such as Tropos, sell mesh nodes for $1,000 and more, but this equipment is highly configurable and has features more suitable for widespread deployments. The recent shake up in the municipal Wi-Fi market will likely drive hardware costs of mesh nodes lower within the next year.

3.1.2 Technology and Issues

Mesh nodes are actually Wi-Fi access points adapted to communicate wirelessly with each using proprietary mesh protocols. A mesh network offers multiple paths from source to destination, and intelligent routing algorithms allow each node to makes a decision on which path to forward packets through the network in order to improve performance. If the link between a pair of nodes along one of the paths is clogged, for example, then the algorithms establish another path that avoids the congested link. Also, if a node goes down, an alternate route is chosen based on the routing algorithms.

When deploying Wi-Fi mesh networks, system integrators can choose among single-radio or multi-radio mesh node equipment. The single-radio models, such as what Tropos offers, uses a solitary 2.4GHz radio for connecting user client devices to the mesh network and interfacing mesh nodes together. This requires both users and node-to-node traffic to share a single radio. With single-radio systems, the radios in neighboring mesh nodes are set to the same RF channel; otherwise, the mesh nodes can’t communicate with each other. With a common channel, a user device transmitting data to a mesh node precludes the mesh node from transmitting data to an adjacent mesh node (and vice-versa). Other vendors, such as Cisco and Strix, offer multi-radio mesh nodes. In the multi-radio case, one radio in the mesh node interfaces users to the mesh network, and an additional radio, operating at a different frequency, provides communications between mesh nodes. This allows traffic between a user and the mesh

node and between the mesh node and neighboring mesh nodes to occur simultaneously.

Which approach is better? One would think that more radios means better performance, and that's generally true. Keep in mind, however, that the single-radio hardware is significantly less expensive as compared to multi-radio versions. This should encourage you to consider the tradeoff between performance and price. If the potentially lower performance of the single-radio system is sufficient to meet requirements, then the single-radio system is the one that you should strongly consider. If requirements dictate higher capacity, then look closely at whether a multi-radio system is really necessary and cost-effective. This just offers some broad direction. Of course one should also think about other parameters, such as security, operational support, and support for newer technologies.

In order to extend the capability of 802.11 serving large-scaled outdoor wireless networks, the 802.11 Working Group kicked off Task Group S in July 2004 to develop the 802.11s standard for mesh networking. 802.11s will provide topology discovery and path selection, something beyond the scope of traditional 802.11 access points. An advantage of 802.11s is that it will enable interoperability among Wi-Fi mesh solutions, which could further reduce costs of Wi-Fi mesh equipment.

The ratification of the 802.11s will likely occur in 2008, but pre-802.11s equipment should start appearing on the market within the next six months with firmware updates later to upgrade the equipment to the final ratified form of the standard. At this point, there's no indication that the majority of Wi-Fi mesh vendors will support 802.11s. Some have proprietary routing methodologies that they will likely want to emphasize over 802.11s, but this could be done similarly to how 802.11b/g access point vendors incorporate functions outside the scope of 802.11b/g. If it's desirable to take advantage of these additional functions, such as enhanced performance, then it's necessary to still use access points (or mesh nodes) from the same vendor. 802.11s will provide value by making it easier to integrate their preferred mesh network into existing deployments

Latency may vary significantly on mesh networks, depending on the number of users and hops that are necessary for moving packets through the back haul network. Roaming and routing delays may offer performance issues, especially for VoIP applications. Even if the data rate between the user and the local backhaul node is kept high, which many of the mesh network vendors claim, the delays across the network may be substantial. A mesh network, though, will likely deliver much better performance than existing 3G systems.

Often the lack of electrical power for mesh nodes in some areas leads to installation delays and unforeseen costs. Some light poles, for example, don't supply adequate electrical power, or occasionally mounting assets, such as roof tops, don't have any readily available power. In these cases, the use of solar panels may be an option for generating power for mesh nodes and backhaul equipment. In this case, the network equipment actually runs off a battery, and the solar panel generates electricity to

recharge the battery and power the mesh node if the battery is charged. Without a battery, there would be no power available at night or when something, such as clouds, obstructs the sunlight.

The use of solar energy is free, which can save electricity costs when running a mesh network. A problem, however, is that the cost of solar panels and batteries can be several hundred dollars for each mesh node. This makes the use of solar power generally only feasible where the cost of installing electrical lines is relatively expensive or where electricity is very unreliable. For example, Chittagong in Bangladesh decided to power some of their mesh nodes with solar energy because electrical power there is not stable enough.

If using solar panels for generating electricity for mesh nodes is appealing, then be certain to investigate average sunlight on a daily basis, and ensure that the solar panels and batteries specified will supply an adequate amount of power for the equipment. This can be a bit tricky since predicting the amount of sunlight may not be accurate enough to satisfy network availability requirements.

3.1.3 Applications

A mesh network is beneficial for areas where it's not feasible to install a traditional wireless LAN consisting of access points. For example, a mesh network approach makes sense to consider for residential and city-wide Wi-Fi networks. The deployment of cabled access points over larger, open areas is a daunting task because of the massive amount of data cabling that requires installation and the countless permissions. Other places where installations are difficult include convention centers, college campuses stadiums, marinas, parks, and construction sites.

3.1.4 Vendors / Products

Several start-ups are offering Wi-Fi mesh products, such as Tropos, BelAir, and Strix. Cisco and Motorola also have mesh solutions. The products are fairly mature, and vendors differentiate themselves by offering advanced mesh protocols and support tools and support for different technologies in addition to Wi-Fi, such as 4.9GHz public safety bands and WiMAX. As mentioned earlier, Meraki offers extremely low-cost mesh node hardware, but the components don't offer flexible configuration needed in larger installations.

3.1.5 Proliferation and Future Outlook

Most municipalities have either deployed or are in the process of deploying Wi-Fi mesh networks in outdoor areas, generally with 95 coverage outdoors and partial indoor coverage. Many large cities (e.g., Chicago), however, are possibly moving away from

Wi-Fi mesh deployments. Recent announcements indicate that Chicago is holding off moving forward with the deployment of a city-wide Wi-Fi network. Deployments are too costly for companies such as EarthLink to bear with somewhat limited user subscription revenues. Municipalities will likely rethink the business model of deploying city-wide Wi-Fi and possibly revive the deployments with partial city funding and a greater emphasis on the value of city applications, such as public safety. The majority of municipalities will likely continue to move forward with Wi-Fi mesh solutions assuming that they based installations on solid ROI for municipal applications.

Mesh networks are not yet ready for wide-scale installation in large enterprise indoor environments, however, mainly because there are no official standards yet for mesh networks. The development of the 802.11s standard could change this, prompting enterprises to deploy a mesh (802.11s) network with 802.11n user interfaces. But, based on the history of the 802.11 group with other standards, such as 802.11n, we'll likely be waiting for a couple years. There are currently dozens of 802.11s proposals, which means that the mesh equipment that you buy today will likely be obsolete after ratification of the 802.11s standard. Enterprises shouldn't invest in this type of technology until standards are firmer.

3.2 WiMAX

WiMAX technologies have been evolving significantly over the past couple years and offers possible competition with Wi-Fi mesh. WiMAX offers many different types of implementations for fixed and mobile solutions in unlicensed and licensed spectrums.

3.2.1 General Attributes

WiMAX includes the following general attributes:

- High performance

  The performance of WiMAX depends on the actual implementation, but most solutions offer data rates in the Mbps range.

- Medium to long range

  Range of WiMAX depends on the actual implementation. Range is generally greater than Wi-Fi due to higher transmit power in some frequency bands.

- Medium power

  WiMAX has similar power requirements as Wi-Fi.

- High to very high cost

Unlicensed-band deployments are relatively low in cost but higher than Wi-Fi due to relatively expensive hardware. Licensed-band deployments are very expensive because of the cost involved with acquiring spectrum and much higher hardware costs for licensed spectrum. This leads to large carriers, such as Sprint, providing WiMAX in licensed spectrum with subscriber-based services.

3.2.2 Technology

WiMAX is based on the following IEEE standards:

- 802.16d (802.16-2004) – only fixed wireless
- 802.16e (802.16-2005) – fixed and mobile wireless

The WiMAX standards were developed for deploying large outdoor wireless networks. WiMAX specifies the use of scalable orthogonal frequency division multiplexing (SOFDM) with operation in both licensed and unlicensed spectrum ranging from 2 to 66 GHz. Lower frequencies, such as 700 MHz, may eventually become available for WiMAX use. Most deployment of mobile WiMAX networks has been done in the licensed (2.5GHz and 3.5GHz) and unlicensed (5.8GHz) bands.

WiMAX operates at a relatively high transmit power, which allows a single mobile WiMAX tower to cover a large area. The big footprint reduces the number of times that a mobile user will roam from one tower to another and lower the chances of having a disruption in service. Some applications, such as voice, are difficult to support when the cell area is smaller, such as with Wi-Fi, and users must roam frequently from one mesh node to another as they do when driving vehicles. WiMAX could indeed reduce rate of handoffs and potential service disruption as compared to higher density of mesh nodes for Wi-Fi coverage, but this benefit will apply on a case-by-case basis. Many wireless applications operate from fairly fixed locations and don't need to roam from one node to another.

Also, similar to Wi-Fi, WiMAX users share bandwidth. As a result, both Wi-Fi and WiMAX users may experience some inconsistency in performance as more or less users are utilizing the system. This is similar to how DSL and cable networks operate.

IEEE 802.16m is underdevelopment. The standard will likely be ratified by 2010 and promises to deliver speeds up to 1Gbps and be backward compatible with 802.16e-2005 solutions. The 802.16m group should wrap up the technology development phase in 2007. Similar to existing mobile WiMAX, 802.16m will use multiple-input/multiple-output (MIMO) antenna technology. The idea with 802.16m, though, is to increase bandwidth by using larger MIMO antenna arrays. The 802.1m group is targeting ratification and finalization of the standard by late 2009.

The advantage of 802.11m to cellular companies is that it will enable the convergence of 3G and 802.16 into a single 4G technology for mobile and fixed applications. This will allow cellular companies to offer service, such as IPTV and VoIP, as effectively over wireless connections as they are today on wired networks. This would lead to competition with existing fixed wireless broadband services currently delivered over cable and telephone lines.

There is often confusion between WiBro, the wireless network being deployed in Korea, and mobile WiMAX. Some think that WiBro is something completely different than WiMAX. Actually, WiBro is based on the same IEEE 802.16e-2005 standard as Mobile WiMAX. WiBro has functionality defined by the Mobile WiMAX system profile, with identical PHY, MAC and Power Classes to Mobile WiMAX. Also, WiBro will be certified using the Mobile WiMAX certification processes and laboratories.

3.2.3 Applications

Fixed and mobile WiMAX provide wireless broadband access to the Internet with MANs and WANs. Momentum is starting to build regarding the delivery of T.V. over wireless networks. For example, the Japan Radio Company (JRC) and Runcom Technologies, Ltd, an OFDMA chipset manufacturer, demonstrated at the CTIA Conference the streaming of a high definition T.V. signal over Mobile WiMAX Base Station equipment and User Terminals based on the 802.16-2005 Standard. This setup was tweaked for high performance, utilizing the highest FFT size (2K) and bandwidth (20MHz) defined in the standard. This resulted in 30Mbps throughput with equipment operating in the 2.5GHz band. This certainly indicates that it's possible to support high definition T.V. over WiMAX. There are certainly practical matters to consider, however, such as impacts of range and numbers of users on the performance of the application. In order to support high definition T.V. delivery, municipalities and system integrators must carefully design the solution to meet desired service levels. If this is done right, then WiMAX could offer some competition to cable operators, especially for mobile users.

3.2.4 Vendors / Products

Many vendors developing WiMAX equipment, such as Motorola, Alvarion, Navini
There is currently no certified mobile WiMAX equipment, but that will likely begin to appear in 2008. The WiMAX Forum completed several mobile WiMAX PlugFests that have focused on key mobility features, such as smart antenna technologies and handovers. As with 802.11 networks, roaming is difficult to get right, even if developers follow the wireless specifications. WiMAX manufacturers seem to be scrutinizing these features. The Plugfest test scenarios could become part of the eventual certification procedures. The Plugfests provide an excellent environment for product manufacturers to gain some practical experience with their products as preparation for actual WiMAX certification.

For a current list of certified WiMAX equipment, refer to the following website: http://www.wimaxforum.org/kshowcase/view.

3.2.5 Proliferation and Future Outlook

There are large carriers deploying mobile WiMAX in licensed spectrum. Sprint-Nextel (teamed with Clearwire) has been working on the deployment of a nationwide mobile WiMAX system in many cities within the U.S. According to Sprint, this WiMAX network will ultimately reach 100 million people across the country by the end of 2008. This is all possible because Sprint has an extensive holding of 2.5GHz spectrum, which covers a very large percentage (roughly 85 percent) of the households in the top 100 U.S. markets. Sprint-Nextel will use 10MHz channels, offering end users with an average 2-4Mbps downlink and 1MBps uplink performance. Peak speeds will likely be higher, similar to broadband cable.

There was initial concern that Sprint-Nextel would deploy a closed WiMAX system, requiring users to purchase a Sprint Nextel interface card that would only work on the Sprint Nextel system. Sprint-Nextel officials have confirmed, however, that Sprint-Nextel is deploying an open Internet model, which allows a Sprint-Nextel WiMAX subscriber to use their mobile WiMAX interface to access a different WiMAX network. If Sprint doesn't have a roaming agreement with the other service provider, the user will still be able to connect and likely pay for limited access, similar to Wi-Fi hotspots today. The costs of this type of roaming across service providers is not know yet, though.

Mobile WiMAX is not suitable yet for unlicensed spectrum due to limited RF interference rejection. The WiMAX Forum is currently working on this, though. Thus, private installations of mobile WiMAX are not feasible or even possible today. Some countries, such as India, are moving forward with WiMAX in unlicensed frequencies, despite the potential for RF interference issues. The regulatory in India has de-licensed 50 MHz of spectrum in the 5.8 GHz band (5.825 to 5.875 GHz) for commercial use. This puts India in line with the majority of the world which also recognizes the 5.8 GHz band as license-free and enables ISPs to offer WiMAX services more easily in India. For example, Sify, a leading Internet and enterprise service provider based in India has already started the process of deploying last mile WiMAX in the license-free 5.8 GHz band throughout various locations in India. Siffy chose Proxim's Tsunami MP.11 WiMAX point-to-multipoint product line as the core communications platform. Siffy has deployed over 700 of the Tsunami base stations and 3,500 subscriber units within 200 cities so far.

These products and systems are just now becoming available. In the background, the IEEE 802.16m Task Group is working on a new mobile WiMAX specification that will offer speeds of up to 1Gbps while maintaining backwards compatibility with 802.16e-2005. The 802.16m group is targeting the finalization of the technology development phase of the standard by the end of 2007 with a ratified standard by the end of 2009.

WiMAX will likely become the dominate wireless MAN (and maybe WAN) standard worldwide. Sprint has recently chosen WiMAX as their 4G cellular technology. Based on announcements made by Intel, we should also start seeing WiMAX integrated into laptops in the next generation of Centrino chips in 2008 and WiMAX in digital cameras and handheld games consoles in 2009. This adds to a growing list of other devices, such as PC cards and mobile phones, that either already or will very soon provide WiMAX interfaces. Whether or not WiMAX will be available in these types of devices by the dates Intel is stating, the wireless industry certainly seems to be gearing up user devices for WiMAX.

The actual proliferation of WiMAX-equipped user devices, though, will depend highly on the magnitude of mobile WiMAX network installations. The wireless industry news is dotted every day with cities around the globe that are in the process of installing and pilot testing mobile WiMAX solutions. This leaves a pretty good impression that WiMAX is coming in a big way, and we'll probably be seeing a large number of WiMAX-equipped user devices soon. For enabling user access WiMAX networks, Sprint is pushing forward with the development of WiMAX client adapters. Sprint has chosen three manufacturers. Samsung will offer PC cards in both single WiMAX mode and dual CDMA 1xEVDO/WiMAX mode. An advantage of the dual mode version is that users can make use of WiMAX where the initial WiMAX networks are available, and then use CDMA in other areas. This would be a good choice for travelers, at least for the foreseeable future. In addition to Samsung, Sprint selected ZTE Corporation and ZyXEL for developing PC cards and modem products.

WiMAX is moving under the 3G standards umbrella. At an ITU (International Telecommunication Union) Radiocommunication Sector (ITU-R) Working Party 8F (WP 8F) meeting in Kyoto, Japan, the group approved the inclusion of WiMAX as a new IMT-2000 terrestrial radio interface. IMT-2000 is the global standard for 3G wireless communications. This means that WiMAX will likely become part of the IMT-2000 family, which could open up additional spectrum for WiMAX applications. Applicable spectrum allocations will be discussed at ITU's World Radio Communications Conference (WRC-07) in October. As part of IMT-2000, WiMAX will also be well-positioned for being part of IMT-Advanced, which will define 4G technologies.

WiMAX service provider roaming agreements are moving forward. Members of the WiMAX Spectrum Owners Alliance (WiSOA) have recently formulated the first WiMAX roaming agreement to provide WiMAX users with "GSM like" roaming between WiMAX service providers. WiSOA also plans to address roaming among WiMAX, Wi-Fi and 3G systems. This is a tremendous step ahead for WiMAX. The first GSM roaming agreement was signed in 1992, and that has been known as one of the major factors that made GSM a worldwide success.

Under the WiSOA roaming agreement, MACH and Trustive will provide turn-key unified clearance, billing, and interconnection solutions. MACH and Trustive will coordinate with equipment manufacturers and service providers to define technical specifications. WiSOA is making it clear that this will be an open process that will solicit input from all

industry stakeholders. Me experiences tell me, however, that this will not be an easy task, but the lessons learned with the implementation of GSM roaming should help smooth out the major problems. At least the primary WiMAX service providers should realize that there are more benefits than not to make roaming work.

The question of whether WiMAX will replace WiFi is highly controversial. The stakes are high. Big companies like Intel are making mobile WiMAX chips, and carriers such as Sprint Nextel are moving forward with large-scale mobile WiMAX deployments. However, there's already a huge installed base of WiFi networks. As a result, it's very unlikely that mobile WiMAX will completely replace WiFi. Users, even if they could, will certainly not hurry to replace their existing WiFi networks with mobile WiMAX in homes and businesses. It's more likely that they will replace the radios in their client devices with a multimode radio that implements WiFi, mobile WiMAX and possibly other technologies. This multi-network architecture is more likely.

3.3 Cellular

Cellular systems have traditionally provided wireless connectivity over very large areas, even worldwide. The evolution of cellular technologies has been relatively slow, however, as compared to Wi-Fi and WiMAX.

3.3.1 General Attributes

Cellular includes the following general attributes:

- Low to medium performance

  Most cellular carriers currently offer 2G and 3G technologies with data rates in the Kbps range. 4G technologies will eventually offer Mbps data rates, but that will likely take several years for the migration to take place.

- Long range

  Cellular systems operate in licensed spectrum blanketing large portions of the World. Users can operate mobile devices in most areas, except possibly larger rural areas.

- Low to medium power

  Cellular offers good battery life, somewhat longer than Wi-Fi devices.

- Very high cost

A cellular system is very expensive to deploy due to high cost for spectrum and hardware. As a result, carriers offer a subscription-based model for client devices. This is effective for rapid deployment, but it could be more cost-effective to deploy private unlicensed band network in the long run, depending on the application.

3.3.2 Technology and Issues

For the past several years, most cellular carriers have been evolving GSM (Global System for Mobile Communications) using GPRS, EDGE, and UMTS technologies:

- GPRS

  GPRS (General Packet Radio Service) brings data connectivity to the GSM market with peak data rates of over 100 kbps. A definite advantage of GPRS is its basis on GSM, which is an open, non-proprietary digital system that supports international roaming capability for a significant installed base of end users throughout the world (primarily in Europe and Asia). In addition, GSM satellite roaming has extended service access to areas where terrestrial coverage is not available.

  GPRS involves overlaying a packet-based air interface on the existing circuit switched GSM network, providing users with a packet-based data service. GPRS facilitates instant connections whereby information can be sent or received immediately without establishing a dial-up connection. To use GPRS, users need a mobile phone or terminal that supports GPRS and a subscription with a mobile telephone network that supports GPRS. In addition to the GSM digital mobile phone standard, the IS-136 Time Division Multiple Access (TDMA) standard, popular in North and South America, will also support GPRS. Initial deployments of GPRS began in 2001 with support of 56 Kbps data rates. Because of higher data rates and expected widespread coverage throughout the world, GPRS has become the primary wireless WAN service.

- EDGE

  EDGE (Enhanced Data rates for Global Evolution) allows GSM operators to use existing GSM radio bands to offer wireless multimedia IP-based services and applications at speeds up to 384 Kbps. EDGE has little technical impact, since it is fully based on GSM, and requires relatively small changes to network hardware and software. Operators do not have to make any changes to the network structure, or invest in new licenses. EDGE uses the same TDMA (Time Division Multiple Access) frame structure, logic channel and 200 KHz carrier bandwidth as today's GSM networks, which allows existing cell plans to remain intact. This makes the technology particularly beneficial to existing operators seeking a way to roll out wideband services rapidly and cost-efficiently across

large areas of existing networks. EDGE has been commercially available since 2001 and is becoming commonplace in mobile devices.

- UMTS

  The UMTS (Universal Mobile Telecommunications System) is the most promising technology to support third generation mobile wireless WANs. This packet switching technology has support from many major telecommunications operators and manufacturers and will likely have transmission rates of over 2 Mbps, enabling the use of video-based applications. The UMTS is part of the Third Generation Partnership Project (3GPP), which is a joint effort between the ETSI and the Association of Radio Industries and Broadcasting. The initial offering of UMTS services began in 2001, but availability has been spreading slowly.

The movement of wireless WANs is progressing toward 4G technologies that will include an IP-based network for supporting integrated voice, data, and video. Carrier selection of 4G technologies will likely be splintered and require use of multi-mode client devices for roaming. For example, Sprint Nextel has chosen WiMAX technology as the basis for their 4G wireless WAN system using Motorola chipsets. Other carriers will likely choose differing technologies to continue to differentiate themselves.

Wireless WANs have limited signal coverage in very rural areas, such as southern Georgia. This leaves significant coverage holes which limits deployment of wireless WAN applications. In these cases, deployments must implement alternative approaches, such as satellite systems.

3.3.3 Applications

Cellular is ideal for wireless MAN or WAN where mobility is necessary and it's not feasibly to install a Wi-Fi or proprietary network. For example, a logistics applications that provides deliver of goods to retail stores in many different areas can make good use of a subscription-based service such as cellular. In this case, it wouldn't be feasible to install a dedicated wireless network in each city because it would be too costly. An application such as this could make use of a city's public Wi-Fi network (if it exists), however. Consider the use of cellular systems for supporting mobile network connectivity where no other wireless network is feasible.

3.3.4 Proliferation and Future Outlook

Cellular systems will continue to dominate the wireless WAN and possibly wireless MAN market. Millions of people have grown dependent on the use of cellular phones for both

work and pleasure. As a result, cellular systems will continue to flourish. The evolution of cellular systems, however, is somewhat slower than Wi-Fi systems, mainly because of the relatively high cost of upgrading systems and appeasing customers. For example carriers, such as Sprint-Nextel, are moving toward 4G (IP-based) technologies, but this could take a decade to fully occur because of the need to replace hardware and allow millions of subscribers to migrate to phones that support 4G technologies.

3.4 Proprietary Solutions

Many existing wireless MAN solutions are based on proprietary radio technology, mostly for line of sight (LOS) and near line of sight (NLOS) applications. Technologies that support mobile applications tend to be based on standards because mobile systems generally support a greater mix of users.

Proprietary solutions for wireless MANs and WANs today mostly utilize OFDM or TDM in the unlicensed frequency bands (900 MHz, 2.4 GHz, 5.4 GHz, and 5.8 GHz). New spectrum allocations are beginning to emerge, though. The 700MHz band will likely become available as FCC mandates digital television broadcasting. It's not clear yet whether the 700 MHz band will become part of a standard, but for the time being, portions of the 700 MHz band that are currently available could be used with proprietary technologies.

The FCC recently upheld a 2005 decision on non-exclusive licensing of broadband wireless services in the 3,650 to 3,700 MHz band. The FCC rejected petitions by Alvarion, Intel, Motorola, the WiMAX Forum, and others who'd opposed the earlier ruling. The FCC calls for using contention-based protocols to allow sharing of the spectrum in the lower 25 MHz of the band. These protocols are how Wi-Fi and other license-free technologies minimize interference among users. The 3,650-MHz band has been used since 1984 for communication satellites throughout the World. Vendors will likely begin selling radios that operate in this band for use in wireless MANs and WANs.

The "White Spaces Coalition" comprised of some market leaders, including Dell, Google, Hewlett-Packard, Intel, Microsoft, and Philips, are pushing for utilization of unused parts of the television analog bands, namely 54MHz to 698MHz, for supporting license-free wireless connections to the Internet. These "white space" frequencies are where T.V. stations are not operating. The beauty of this band is that it's lower in frequency as compared to Wi-Fi, WiMAX and cellular, which affords greater range. This keeps node density low, which of course equates to lower cost infrastructure. The bandwidth potential in the T.V. band is also relatively wide, which can possibly support higher performance.

Several legislators, including Senator John Kerry, are pushing the FCC to move forward with opening up the unused T.V. channels for wireless computer connectivity. The FCC has already approved the operation of fixed unlicensed devices in the white spaces starting February 19, 2009, which is the day after analog T.V. broadcasting will end. The

FCC is currently seeking comments on mobile equipment. U.S. Representative Inslee has recently introduced a bill instructing the FCC to finish the approval process of mobile devices and allow operation of mobile devices in white spaces no later than February 18, 2009 and to establish technical requirements that protect incumbent licenses from harmful interference. This is a technology worth watching because it could provide additional options for proprietary or standards-based wireless MANs and WANs.

3.5 Satellite

Satellite-based wireless WANs provide global coverage for the transmission of voice, data, and video. The satellite is a platform in geostationary orbit that hosts a series of transponders acting as signal repeaters. The geostationary orbit places the satellite directly over the Earth's equator; therefore, earth-based satellite stations in the Northern Hemisphere orientate their antennas (satellite dishes) toward the satellite in the southern horizon. The transponders receive signals directed to the satellite on the uplink from earth stations and broadcast the signals back to earth on a downlink frequency with a fairly broad propagation pattern. This enables stations located over a very wide area to receive signals transmitted by other stations. The advantage of a satellite system is certainly wide coverage, which is typically worldwide. They offer moderate data rates (typically near DSL speeds) for 2-way, full-duplex operation. Companies such as Hughes offer applicable service for $40 to $50 per month.

Because of the extremely wide coverage area, consider offering satellite system solutions to applications in the transportation area of the logistics market. Vendors provide satellite-based transceivers that can be mounted on trucks to provide continuous, worldwide, data connectivity with a centralized information system.

4. Roaming

Roaming includes several different levels: access point, subnet, and ISP/carrier. The following sections discuss the issues and potential solutions of each of these levels of roaming.

4.1 Access Point Roaming

In general, wireless technologies provide access point roaming protocols. For example with Wi-Fi networks, the client radio makes a decision to handoff to the next access point when retransmissions and received signal levels indicate a need to handoff. A decision to handoff too soon generally leads to skipping back and forth between access points. As a result, vendors generally choose to dampen the handoff process and wait until it's absolutely necessary to handoff to the next access point.

Based on extensive roaming tests that Wireless-Nets has completed, the dampening of the handoff process leads to sluggish roaming. In a test with results comparable to other tests that Wireless-Nets has completed, we configured one access point (AP-1) set to channel 1 and the other access point (AP-2) set to channel 6. Other settings were default values, such as beacon interval of 100 milliseconds, RTS/CTS disabled, etc. The access points were installed in a typical office facility in a manner that provided a minimum of 25dB signal-to-noise ratio throughout each access point's radio cell, with about twenty percent overlap between cells. This is somewhat the industry standard for wireless voice applications. The roaming client in this test was a laptop equipped with an internal Centrino Wi-Fi radio (Intel 2915ABG).

While standing with the wireless client within a few feet of AP-1, we used AirMagnet Laptop Analyzer (via another Wi-Fi card inserted into the laptop's PCMCIA slot) to ensure that that the laptop was associated with AP-1. We then initiated a FTP transfer of a large file from the server to the laptop and started measuring the 802.11 packet trace using AirMagnet Laptop Analyzer. With the file downloading throughout the entire test, we walked toward AP-2 until directly next to it. With the packet trace, we were able to view the exchange of 802.11 frames, calculate the roaming delay, and see if there was any significant disruption to the FTP stream.

Once the client radio decided to re-associate, it issued several 802.11 disassociation frames to AP-1 to initiate the re-association process. The radio then broadcasted an 802.11 probe request to get responses from access points within range of the wireless client. This is likely done to ensure that the client radio has up-to-date information (beacon signal strength) of candidate access points prior to deciding which one to re-associate with. AP-2 responded with an 802.11 probe response. Because the only response was from AP-2, the client radio card decided to associate with AP-2. As expected, the association process with AP-2 consisted of the exchange of 802.11 authentication and association frames (based on 802.11 open system authentication).

The re-association process took 68 milliseconds, which is the time between the client radio issuing the first dissociation frame to AP-1 and the client receiving the final association frame (response) from AP-2. This is quite good, and we've found similar values with other vendor access points. The entire roaming process, however, will interrupt wireless applications for a much longer period of time. For example, based on my tests, the FTP process halts an average of five seconds prior to the radio card initiating the re-association process (i.e., issuing the first disassociation frame to AP-1). We measured 802.11 packet traces indicating that the client radio card re-retransmits data frames many times to AP-1 (due to weak signal levels) before giving up and initiating the re-association with AP-2. This substantial number of retransmissions disrupted the file download process, which makes the practical roaming delay in my tests an average of five seconds! The Centrino radio card we tested is notorious for this problem, but we've found this to be the case with most other radio cards as well.

Every model radio card will behave differently when roaming due to proprietary mechanisms, and some cards will do better than others. Keep in mind that roaming may take much longer than expected, so take this into account when deploying wireless LAN applications, especially wireless voice, which is not tolerant to roaming delays exceeding 100 milliseconds. The use of wireless middleware can also help accommodate patterns of broken communications between the client and the server caused by roaming delays.

The finalization and proliferation of IEEE 802.11r and 802.11k will have a positive impact on access point roaming issues. 802.11r will provide seamless roaming between access points. The main application for 802.11r is for providing effective roaming for VoIP and security mechanisms. 802.11r provides functions for determining QoS and performing security protocol handshakes before handoffs occur to avoid delays after handoff. Ratification of 802.11n will likely occur in mid to late 2008. 802.11r will certainly improve use of VoIP over Wi-Fi networks.
802.11k works in conjunction with 802.11r by providing information to discover the best available access point for handoff purposes. Consider incorporating 802.11r and 802.11k into VoIP and security applications.

4.2 Subnet Roaming

As a wireless client device on a Wi-Fi network (or any other IP-based network) roams from one IP subnet to another, the client device must obtain a valid IP address for the new subnet. The client device can make use of DHCP to obtain the IP address, but this is not effective when supporting mobility. DHCP is not designed to renew addresses when crossing subnet boundaries. As a result, many enterprises configure wireless LANs on a single subnet. This may work in a private network, but the subnet roaming issue resurfaces when the client device needs to roam to another network. Consider the use of wireless middleware for applications that are affected by subnet roaming issues.

4.3 ISP/carrier roaming

With Wi-Fi hotspots, there is very limited among wireless ISPs. The Wi-Fi Alliance had tried developing standards several years ago to make wireless ISP roaming seamless, but the group later disbanded due to significant incompatibility among differing access controllers. In general, roaming from one Wi-Fi wireless ISP to another is virtually non-existent.

The roaming from one particular cellular carrier and another, however, is fairly good due to availability of cellular phones with multiple radio technologies and roaming agreements and applicable systems in place between cellular carriers. When a roam takes place between carriers while a user is actively participating in a call, the calls generally drop because of roaming delays. A very small percentage of cellular calls, though, are made while traversing carrier boundaries, so dropped calls based on this reason seldom occur. Most carriers implement multi-homing for calls taking place within the home carrier network. In this case, a cell phone will have connections to multiple cell towers, which significantly decreases the rate of dropped calls in the home network.

The Unlicensed Mobile Access (UMA) group provides a roaming solution between various technologies. UMA provides access to GSM and GPRS mobile services over unlicensed spectrum technologies, including Bluetooth and 802.11. This can enable subscribers to roam and handoff between cellular networks and public and private unlicensed wireless networks using client devices supporting multiple network modes Primary participants are major players in the cellular industry (Alcatel, BT, T-Mobile, RIM, etc.). It’s too early to tell how well this technology will proliferate.

3G / Wi-Fi bridges offer a solution for roaming among carrier-based systems and Wi-Fi as well. For example, Autonet Mobile and Avis are partnering to offer Wi-Fi Internet access to car renters via 3G / Wi-Fi bridges installed in Avis rental cars. The bridge provides a Wi-Fi hotspot inside and within approximately a hundred feet of the vehicle, making the automobile a highly mobile hotspot. The bridge also connects to a cellular provider’s 3G network, which supports connections to the Internet. This is a great application for car renters. For example, a passenger might need to download an important file while traveling to a meeting. It can also lead to use of location-based applications when combined with a GPS.

5. Location-Based System Solutions

This section discusses the applications and technologies associated with location-based systems.

5.1 Applications

Location-based systems enable the following applications:

- Local information pushing. In this case, a positioning system sends valuable information to a client based on the client's location. For example, a processing plant may push workflow information to employees regarding operating and safety procedures relevant to their locations in the plant. The positioning system tracks each employee and has knowledge of the floor plan of the facility as well as the procedures. When an employee steps within a defined perimeter of a particular area, such as a packaging department, the positioning system displays on a person's PDA the steps on for the work needing to be done in that area. This significantly increases efficiency and safety by ensuring that employees follow carefully designed guidelines.

- Centralized tracking. In some cases, it's advantageous to keep tabs on the location of objects. With centralized tracking, a positioning system continuously stores and displays the position information to an operator. This leads to more effective management of assets. As an example, a hospital can track patients in an operating room to analyze and remove bottlenecks in the flow of work to increase throughput and ultimately the quality of care. Historical workflow data and asset usage per location can provide invaluable information in optimizing a variety of processes. .

- Decentralized tracking. This goes a step further than centralized tracking by having the centralized station broadcast client positions to all clients. As a result, each client knows the position of other clients in relation to themselves. With this capability, it's possible to exploit the location of other users to make better decisions, such as in emergency response to natural disasters and terrorist attacks. In these situations firefighters, for example, can better spread out and make decisions when responding to a massive fire when they can know the position of each of the other firefighters.

- Navigating. Positioning systems make navigation simple by supplying the x-y coordinates of a client superimposed onto a map of a particular area. When knowing their location, a user discovers how to proceed to a specific location in a timely manner. Libraries, for example, have found this form of positioning very useful for patrons. A person looking for a book carries a PDA that offers an electronic map of the library and the person's location. After entering book

information, the PDA clearly illustrates the place of the book on the map. After following some simple directions that the PDA offers, the patron finds the book much faster, without the help of library staff.

5.2 Technologies

The following sections describe the various technologies that location-based systems implement.

5.2.1 Global Positioning System (GPS)

GPS is commonly deployed in a variety of devices, such as handheld GPS receivers that provide latitude and longitude as well as moving maps for navigating airplanes and automobiles. The GPS consists of satellites in located geostationary orbit around the Earth. These satellites remain in a fixed position relative to the ground and continuously transmit coded beacon signals. A GPS receiver located on a client receives simultaneous signals from multiple GPS satellites and uses a time-based approach for calculating position. The successful reception of at least three satellite signals is enough to calculate x-y coordinates. With a greater number of satellite signals, however, accuracy is better, and it's even possible to determine elevation. Position accuracy is generally within several feet.

GPS solutions calculate range between satellites and receivers based on propagation time and the fact that signals travel at the speed of light. With knowledge of range between itself and several satellites, a particular GPS receiver can calculate its position. The range is great enough for this approach to work fairly well with available clock accuracies. With positioning systems installed indoors, propagation delay is so small that it's difficult for most clocks to measure to determine range within accuracies consistent with the actual ranges.

An issue is that GPS signals are relatively weak, making it only usable in areas with an unobstructed path between the GPS receiver and the sky. In fact, GPS is not usable at all inside buildings. Tree foliage also significantly limits GPS signals. Even narrow areas surrounded by tall buildings, such as within large cities, will impair signal reception. In order to enhance coverage of GPS, the Assisted GPS (A-GPS) systems are available. A-GPS use ground-based GPS servers to extend range in large cities and in some cases inside facilities. A-GPS solutions, however, are very costly to deploy.

As with most other positioning technologies, GPS requires a dedicated chipset in the client device. This entails the installation of GPS circuitry, which adds to the expense and complexity of the user device.

5.2.2 Real Time Location System (RTLS)

A RTLS includes radio frequency identification (RFID) scanners installed throughout a facility that interrogate either active (radio transceivers) or passive tags that attach to objects. Active tags must use batteries and allow up to twenty feet range between the scanner and the tag. Passive tags don't use batteries, and they receive energy when being scanned. The radio waves emitted by an RFID scanner energize a passive tag long enough for the tag to transmit its code to the scanner. Passive tags, however, must be relatively close (within inches) to the scanner. As a result, radio transceivers are the most common type of RFID tag found in positioning systems.

RFID tags contain electronic codes that identify one tag from another. A centralized station stores the tag codes that the scanners collect. Because the scanners are placed in known positions throughout a facility, the centralized station is able to identify and display the location of each tag (and of course the client device that the tag corresponds with).

RFID systems determine position based merely on the presence of the object in a particular area, within range of a RFID scanner. When a person wearing a RFID tag enters a room, for instance, the system indicates the existence of that person as soon as it detects the tag's signal. As a result, the accuracy of a RFID system is highly dependent on the positioning of the scanners. One scanner per room only provides location accuracy to the size of the room.

The cost of installing additional RFID scanners for finer tracking is cost-prohibitive for most applications because of the relatively high cost for multiple scanners per room. As a result, it's not practical to use a RFID to provide real-time tracking of objects. In addition, the deployment of a RFID system over a large campus or enterprise area is very expensive because of the need for installing a multitude of scanners completely separate from the corporate network. Also, changing the layout of a manufacturing plant or moving walls in an office requires remounting and rewiring of the RFID readers. This is a major problem in frequently changing environments or in complex indoor environments.

An issue with the proprietary hardware used with RFID systems is that the resulting deployments are difficult and costly to scale up to support a larger numbers of users. Proprietary hardware is usually only available from a single vendor, making equipment prices higher than standards-based solutions. In some instances, vendors may even go out of business, making the hardware obsolete. Standards-based solutions are certainly preferable in order to reduce these costs and operational support risks.

In addition, some RFID systems operate in the same frequency band as wireless LANs, which poses RF interference issues for companies needing wireless LAN connectivity for mobile data applications. It's nearly impossible to ensure that the RFID system and the wireless LAN are operating on different, non-interfering channels throughout the

facility. The continual transmissions taking place in a RFID system causes a decrease in throughput in the nearby wireless data network.

5.2.3 Wi-Fi-based Positioning

The critical issues of the positioning technologies discussed so far include the proprietary nature of the scanners and tags, needs for an infrastructure that is completely separate from a company's data network, and limited real-time operation. These common attributes make the systems costly to deploy, scale, and support. In some cases, the negative characteristics make the systems unsuitable for highly mobile, location-aware or tracking applications found in hospitals, warehouses, manufacturing plants, universities, and enterprises.

Over the past few years, Wi-Fi has been proliferating as the primary standard for wireless LANs in company facilities and homes worldwide. With the widespread adoption of wireless LANs, Wi-Fi is an ideal technology as the basis for positioning technologies. A Wi-Fi-based positioning system, such as the one offered by Ekahau, is completely software-based and utilizes existing Wi-Fi access points installed in a facility and radio cards already present in the user devices. Ekahau also offers a WiFi-based radio tag that uses industry standard components that adhere to the 802.11 standards. This approach allows for the use of commercial off-the-shelf hardware and drivers to produce a standards-based radio tag that can communicate bi-directionally.

Ekahau's standard Wi-Fi-based solution is completely vendor-agnostic in terms of hardware. Wi-Fi cards come in many different form factors, such as PC Card and Compact Flash as well as built into newer PDAs, laptops, tablet computers and a variety of other purpose built devices. Thus, a standard Wi-Fi-based positioning system can realize any type of location-aware application that involves PDAs, laptops, bar code scanners, voice-over-IP phones and other 802.11 enabled devices. For embedded solutions, there is no need for the client to include a specialized tag, transmitter, or receiver. Position accuracy is generally less than ten feet, depending on the number of access points in range of the client device.

Because of the entire use of standards-based hardware, such as 802.11b, 802.11g, and 802.11a, a standard Wi-Fi-based solution rides the installed based and economies of scale of the networks and end user devices that are proliferating today. Without the need for additional hardware, a company can install the system much faster and significantly reduce initial and long-term support costs. A common infrastructure supports both the data network and the positioning system, something companies strive for. The positioning system works wherever there is Wi-Fi coverage.

In addition to cost savings in hardware, a standard Wi-Fi-based positioning system significantly reduces the potential for RF interference. The total Wi-Fi positioning system shares the same network along with data, so there is no additional installation of a separate wireless network (as RFID requires) that causes RF interference with the

existing wireless data network. Most wireless LANs are underutilized, leaving plenty of capacity available for location-aware applications. Consider a Wi-Fi network as the potential infrastructure for positioning systems.

6. Middleware Solutions

The traditional components of a wireless network (e.g., radio cards and access points) provide a path for data to flow between the end user device and a wired network that has connectivity to the host or server. In order to communicate effectively, wireless systems must also include connectivity between the end user and the application software and system databases. The following sections describe each of the primary methods for providing wireless application connectivity.

6.1 Terminal Emulation

Terminal emulation software makes an end user device appear as a terminal to application software running on a host-based operating system, such as Unix and AS/400. For example, VT (Virtual Terminal) emulation software interfaces with an application running on a Unix host. Likewise, 5250 emulation software will interface with an application running on an IBM AS/400. Terminal emulation software on wireless appliances generally communicates with the host using Telnet over TCP/IP protocols. After a connection is made with the host, the application software residing on the host can send display information (such as log on prompts, menus, and data) to the appliance, and keyboard strokes will be sent to the application. Thus, the software on the host provides all application functionality.

Terminal emulation provides the following advantages:

- Lower presumed initial costs: Terminal emulation can be less expensive initially than implementing other approaches if only taking into consideration the costs of the terminal emulation software. This is often the mistake that some customers make when cost-justifying a wireless LAN implementation. They are not aware that other elements, such as potential host application modifications and support issues, can increase the cost of a terminal emulation-based system. As a result, it is important that a solution provider fully assess these costs associated with terminal emulation before proposing a solution to the customer.

- Central application software control*:* With terminal emulation, all application software is updated only at the host, not the individual appliances. All users will automatically take advantage of changes to the application without needing updates to the software on the appliance. This makes configuration management much easier, especially when there are hundreds of appliances.

- Common technical expertise: If the end user organization has an existing terminal/host system, then the company will likely have the core competency to implement terminal emulation-based wireless systems.

Terminal emulation provides the following disadvantages:

- Legacy code changes: Most host-based application screens have been written to fit a standard desktop terminal screen. When integrating a wireless terminal, programmers must often rewrite the host application code to present screens small enough to fit in the smaller displays of the wireless terminals. If printing is necessary from the end user device, programmers will also need to embed the print streams of the particular printer in the application on the host. The problem is that it is not always practical to modify the host application software. For example, the vendor supplying the application software may not permit such changes to be made. In this case, the solution provider is severely limited in adding new functionality to the application.

- Inflexible programming environment*:* When developing or modifying the application on the host, the terminal emulation specifications (e.g., VT200, 5250, and 3270) limit the control of the end user device from the host-based application. This often constrains what programmers can do when adding functionality.

- Limited support for migration to client/server systems: Terminal emulation software does not interface directly to databases, making it unsuitable for client/server implementations. Thus, terminal emulation enables users to access only the screens that the host application provides.

- Difficulty in supporting the end user devices: With standard terminal emulation, there is no effective way to monitor the performance of the wireless appliances, making it difficult to troubleshoot wireless network problems. In addition, terminal emulation protocols were designed to operate over wired networks, not wireless networks that are prone to loss of connections due to RF interference and inadequate coverage from time to time. As a result, wireless terminals can lead to erratic information stored in the application software or databases when transactions are not fully completed due to a loss of connectivity over the wireless network.

- Significant effect on wireless networks*:* With terminal emulation, all screens and print streams must traverse the wireless network, affecting the performance of the overall system. In addition, terminal emulation utilizes TCP (transmission control protocol) to maintain a connection with the host, and TCP does not operate efficiently over wireless networks.

Some companies implement terminal controllers that provide an efficient interface between the end user device and the host. The terminal controller provides effective management of the wireless end user devices while maintaining constant connections with the host. The problem with these controllers is that they generally do not support forms of connectivity other than terminal emulation. For example, they do not support interfaces to databases via ODBC, as many of the newer end systems require.

The implementation of terminal emulation over wireless networks was very common throughout the 1990s; however, companies are now replacing many of these host-based systems with client/server systems. Client/server systems consist of a client software element that generally runs on the end user devices and a database located on a server. The migration from terminal/host systems to client/server is eliminating the need for terminal emulation. Instead, customers need other forms of connectivity software as explained in the following sections. Consider other forms of connectivity in order to support the interoperability with client/server systems.

6.2 Browser-based Approaches

The explosive use of mobile phones, PDAs, and the Internet is prompting the rapid development of browser-based application connectivity technologies and standards for interfacing with information and applications at websites on the Internet and company intranets. A major problem with accessing the web wirelessly today, however, is that most web pages are written to display information on large desktop screens over relatively high bandwidth physical connectivity. These pages don't work well over lower data rate wireless connections and small handheld device screens. In addition to solving these performance issues, the wireless Internet revolution is fueling the need for interoperability in the way mobile devices access web-based information.

Browser-based application connectivity provides the following advantages:

- Common open interface*:* The common open interface to applications and information leverages skills needed to develop applications for wireless users.

- Central application software control: With intranet-based connectivity, all application software is updated only on the web server, not the individual end user devices. As with terminal emulation, all users will automatically take advantage of changes to the application without needing updates to the software on the end user device.

- Strong support for client/server systems*:* Intranet-based connectivity software (i.e., web browser) offers a thin client front end to an application residing on the server.

Browser-based application connectivity provides the following disadvantages:

- Extensive web page changes. As with terminal/host systems, most existing websites have pages that are designed to occupy larger desktop screens. As a result, existing pages must be rewritten to work effectively on the smaller screens of wireless end user devices. Developers must pay close attention to usability issues with smaller screens than they may with larger desktop-sized screens.

- Potential effect on wireless network performance: Web-based connectivity can consume large amounts of the limited wireless bandwidth, depending on the type of application. For example, the browser on the appliance may point to a web page containing large graphic files that must be sent from the server to the appliance. Most intranet-based implementations may also utilize TCP to maintain a connection with the host. As mentioned before, TCP does not operate efficiently over wireless networks.

Many end user companies within the logistics supply chain are deploying intranets and Internet-based applications. It is very likely that these end users will benefit from access to these applications via mobile devices such as cell phones, PDAs, data collectors, and portable computers. As a result, consider developing web browser interfaces for their end user devices.

6.3 Direct Database Interfaces

Some companies develop customized versions of application software that run on the end user device and interfaces directly with a database on a server via ODBC (open data base connectivity) or proprietary protocols. With this configuration, the software on the end user device generally provides all application functionality. The application software with direct database connectivity generally uses TCP/IP software as a basis for communicating with the server. Some programmers refer to this form of development as socket programming.

Direct database interfaces provide the following advantages:

- Flexible programming environment*:* Direct database connectivity enables the programmer to interact directly with database records, rather than be limited to what the application software on the host provides (as is the case with terminal emulation). This provides a great deal of control for a solution provider to add functionality to the application.

- A moderate amount of programming needed to interface new appliances with existing applications*:* With direct database connectivity, developers must often create a program that runs on the appliance to interface with the existing database. This requires the developer to understand how to write software that interfaces with the specific display, keyboard, scanner, and peripherals of the applicable end user device.

- Distributed application software control: New releases of application software must be installed on each of the end user devices when deploying upgrades to the application. This can be a tedious task if there are more than just a few end user devices. One method that helps overcome this problem is to store the current version of the end user device application software on a server and have the application software running on the appliance compare its current version

with the one located on the server. If the one on the server is a newer release, then the application software on the end user device can automatically download and install the newer version of software over the wireless network. In addition, modifications to the central database structure may require changes to the application software on the appliance. Care must be taken to ensure these application changes are made to guarantee the application works properly.

- Good support for client/server systems*:* Direct database connectivity fits well into the client/server system model, enabling programmers to develop front-end applications that run on the appliance.

Direct database interfaces provide the following disadvantages:

- Application size limited to the amount of appliance memory*:* With direct database connectivity, the end user device must have sufficient storage for the application software.

- Wireless network impacts*:* With direct database connectivity, only the database inquiries and data records must traverse the wireless network, making efficient use of the wireless network performance in terms of data transfers. All print streams and screen interfaces can be handled within the end user device. Most direct database implementations, though, utilize TCP to maintain a connection with the host. As mentioned before, TCP does not operate efficiently over wireless networks.

Because of the poor performance of TCP over wireless networks, avoid the direct database form of connectivity.

6.4 Wireless Middleware

Wireless network middleware is an intermediate software component generally located on the wired network between the wireless end user devices and the application or data residing on the wired network. Middleware client software runs on the end user device and communicates using efficient (often proprietary) wireless protocols with middleware software (controller) residing on a platform such as Unix or Microsoft NT Server. The middleware controller software then communicates with host applications and databases over a wired connection.

With the continuing need to support bandwidth-intensive applications, companies will implement wireless middleware as part of their wireless network solution with the goal of increasing performance. To accomplish this, middleware attempts to counter wireless network impairments, such as limited bandwidth and disruptions in network connections. Middleware enables highly efficient and reliable communications over a wireless LAN,

while maintaining appropriate connections to application software and databases on the server/host via the more reliable wired LAN.

Traditionally, middleware suppliers could only enable a limited set of end user devices and only interface with a specific end system. Presently, suppliers are striving toward making middleware as open as possible by incorporating many different end user devices, hosts, and servers. End user companies generally select middleware software based on the ability to interface with their specific end systems, which tend to be IBM AS/400s, Microsoft 2000 Servers, or Unix hosts. In addition, end users generally want wireless middleware software capable of supporting a variety of end user devices provided by different vendors. This minimizes limitations when adding additional end user devices in the future.

Wireless middleware can provide these features/advantages:

- Optimization techniques: Many middleware products include data compression at the transport layer to help minimize the number of bits sent over the wireless link. Some implementations of middleware use header compression, where mechanisms replace traditional packet headers with a much shorter bit sequence before transmission.

- Effective migration to client/server networks: Through middleware software, an end user device can be enabled to communicate with both host-based applications and databases residing on servers. The ability of wireless middleware to interface with a wide variety of end systems enables the migration from terminal/host to client/server systems, without affecting the end user device functionality.

- Intelligent restarts: With wireless networks, a transmission may be cut at midstream due to interference or operation in fringe areas. An intelligent restart is a recovery mechanism that detects when a transmission has been cut. When the connection is reestablished, the middleware resumes transmission from the break point instead of at the beginning of the transmission.

- Data bundling: Some middleware is capable of combining (bundling) smaller data packets into a single large packet for transmission over the wireless network. This is especially beneficial to help lower transmission service costs of wireless WANs. Since most wireless data services charge users by the packet, data bundling will result in a lower aggregate cost.

- Store-and-forward messaging: Middleware often performs message queuing to guarantee message delivery to users who may become disconnected from the network for a period of time. Once the station comes back online, the middleware will send the stored messages to the station.

- Screen scraping and reshaping: The development environment of some middleware products permits the developer to use visual tools to "scrape" and "reshape" portions of existing application screens to more effectively fit within the smaller display of data collectors.

- Operational support mechanisms: Some middleware products offer utilities and tools to monitor the performance of wireless end user devices, enabling MIS personnel to better troubleshoot problems.

- Application development tools: Some middleware packages also include tools for developing applications that operate independently from the end user device and host application. This allows a company to add application functions to legacy systems.

Wireless middleware provides the following disadvantages:

- Higher initial costs: The wireless middleware software and associated hardware platform is relatively expensive compared to other forms of application connectivity. Wireless middleware list prices range from US $5,000 to U.S. $15,000 per server plus additional license fees for each end user device. The solution provider must clearly cost-justify the benefits of purchasing a wireless middleware-based solution for customers.

- Lack of standards: There are many proprietary wireless middleware products, with each offering a different form of operation and development/integration environment. This often requires developers to learn a somewhat foreign form of programming. Also, end users must often only utilize end user devices that have been integrated into the chosen middleware software.

Wireless middleware is often a significant differentiator for companies selling wireless solutions. Based on the features described above, wireless middleware offers significant benefits that easily outweigh the disadvantages. As a result, consider the inclusion of a full-featured wireless middleware product in their product line that interfaces with a wide variety of standard and proprietary wireless networks, end user devices, and host and servers. This would provide an integration tool that adds value in nearly any implementation.

There is lots of variance in the feature sets that different middleware products have, making it difficult to decide upon which vendor to choose. One should start the selection process by analyzing the application’s environment, and then define which middleware features are most important. Be sure to identify all types of end systems that will be part of the applications and ensure that the middleware has the appropriate hooks. For example, the middleware will likely need to incorporate 5250 terminal emulation if there’s a need to be interfacing with AS/400 applications. Just as important as the end systems are the mobile client devices. Bear in mind that middleware vendors produce client software for a limited number of device types. If there’s a need to support a

specific smart phone, for instance, ensure that the middleware includes client software for that device. The middleware client is generally not portable because of the need to match the applicable operating system, screen size, and keyboard.

The following are vendors that provide wireless middleware solutions:

- Connect - www.connectrf.com
- Iona - www.iona.com
- Netmotion – www.netmotionwireless.com
- Nettech Systems - www.nettechrf.com
- Wavelink – www.wavelink.com

7. Management

This section discusses various management topics related to wireless solutions.

7.1 Network Monitoring

Network monitoring continuously measures attributes of the wireless LAN. This plays a key role in proactively managing the network in a way that enables smooth upsizing to support a growth of users and ability to solve issues before they hamper performance and security. When planning operational support for a wireless LAN, consider monitoring the following elements:

- Performance. Continually measure the usage of access points to provide valuable information necessary to properly scale the wireless LAN as user traffic changes. The utilization of access points acts as a gauge to indicate when additional access points, access controllers, and Internet bandwidth are necessary. In addition, network monitoring should also keep an eye on sources of RF interference and raise flags when the interference is high enough to cause significant degradation in throughput.

- Coverage. Alterations made to a facility, such as addition of new office partitions and influx of additional employees, cause attenuation and make radio waves propagate differently. This causes coverage of the wireless LAN to change, often limiting wireless user access to the network. In extreme situations, an access point may become inoperative due to a broken antenna or firmware fault, which requires maintenance or rebooting before users are able to associate with the access point.

  Because most companies deploy wireless LANs having access point range boundaries that radically overlap, however, total loss of connectivity may not occur. Instead, users experience lower performance in certain parts of the facility. In this case, users tend to not complain to strongly to the IT group about the problem, making it tricky for network administrators to determine whether an access point is down. Network monitoring is certainly a remedy to this problem.

- Configuration settings. When installing access points, several configuration parameters, such as SSID, RF channel, and transmit power, are set. It's important to monitor these configuration settings over time. Network managers should be aware of the configuration of all access points in order to facilitate effective updates to the network. Documentation of the access point configurations can be easily lost. Monitoring of the configurations enables accurate, centralized records of the setting values.

In addition, a hacker may attempt to reconfigure an access point to a default configuration that is insecure and comprises the security of the network. Tools should continuously monitor all of the access points in the network and alert the IT staff if anything strange is going on. The IT staff can set the performance and security thresholds at any value they wish and change them at any time. Some software packages also have auto-repair features, which automatically return the access points to their proper settings if someone tampers with the settings or a maintenance person reboots the access point due to a malfunction.

- Rogue access points. Network monitoring should identify the presence of rogue access points to ensure there are no open, unprotected entry points into the corporate information system. This can be done by placing monitoring pods through out the facility to detect unauthorized access points, or monitoring can (ideally) be done over the Ethernet side of the network. Most vendors making wireless LAN management tools now include rogue access point detection.

If possible, a company should integrate the network monitoring function into tools in use for monitoring the existing Ethernet corporate network. Most access points offer simple network management protocol (SNMP) that provides an interface to existing wired network monitoring tools.

7.2 Device Management

One should carefully plan the integration of wireless devices into a company, with an eye on deploying an effective management system. This proactive approach should take advantage of standards and best practices, which includes the technologies and support mechanisms that ensures a secure, reliable, and cost-effective solution. The deployment of an effective mobile device management strategy is critical for achieving expected ROI.

The following are device management elements that you should consider:

- Software management. It's normally not feasible to have users install new software as it becomes available. This generates more problems than the time it saves of having an IT person install the software. Also, a company certainly can't have a hundred mobile devices brought into a central location from the field to facilitate the installations. That just isn't practical. Instead, look for methods in management systems for centrally distributing and installing software applications over the network.

- Security management. With mobile devices, security becomes something that requires special attention. The mobile management solution chosen should include up-to-date methods for detecting and eliminating viruses on user devices. Also, device wiping functions, which can purposely destroy data and application

software on mobile devices, is important to safeguard sensitive information in case the device is lost or stolen.

- Configuration management. One can't rely on all users to properly configure mobile devices with settings that comply with company policies. Thus, the management system should have features for automatically configuring devices from over the network. This saves time and eliminates human errors.

- Inventory management. The management solution should be able to automatically keep track of the number and type of mobile devices in use at the company. This is important to properly plan support staffing and analyze the effectiveness of mobile technology. Also, features that identify usage levels of various applications are also beneficial when allocating funding for supporting the different applications.

- License management. Licenses can be a bit tricky to manage through manual means. As a result, ensure the management solution has functions that automatically identify the need to renew licenses on user devices. This saves a lot of time and keeps a company out of legal trouble by ensuring proper compliance.

- Remote control. This is helpful when a user desperately needs someone to help them through a particular problem. From a central location, an IT person can remotely take control of the user device and install software patches, make corrective settings, and troubleshoot the device.

- Data management. In order to recover from lost, stolen, or broken user devices, a company must keep a central repository of application and user data. That way the data is not lost, and the user can startup faster with a new device right where they left off.

8. Common Trends

The following sections discuss the commons trends of wireless networks:

- Broader Base of Applications

  A major trend within wireless LAN markets is that end user organizations are continuing to integrate wireless LANs into their corporate information systems to support a broader base of applications. Because of newer higher speed standards and lower prices, it is practical and cost effective for companies to implement interoperable wireless LAN solutions for a variety of mobile, portable, and stationary applications. For instance, wireless video surveillance is beneficial for many industries. San Mateo County, for example, had installed Wi-Fi video cameras around the court house while the Scott Peterson trial was taking place. With this system, security officials could keep a continual eye on crowds and their behavior. In addition, public facilities, such as hotels and shopping malls, utilize Wi-Fi cameras to watch over shopping areas, inside elevators, and exit doors. Enterprises are also taking advantage of Wi-Fi cameras to monitor lobby entrances and parking lots.

- Higher Performance

  Because of the higher data rates, companies are not just implementing wireless LANs for the sole purpose of supporting a single application, such as a bar code system. Instead, they are taking advantage of high bandwidth in newer wireless LAN technologies to support multiple mobile information system applications, which decreases the time to recoup investments in the RF hardware and associated software. In many cases, end user companies will not know what wireless requirements they will have beyond the first year. For example, a company may implement the initial wireless LAN to support a bar-coding application with the thought of using the same wireless LAN to support “future applications.” End users may not be able to realize and plan additional wireless applications until they have used the initial wireless LAN for a period of time. Once they see the wireless LAN in operation, they are likely to define additional applications. Clearly, vendors need to supply wireless LAN solutions that will scale easily to meet greater demands for bandwidth. End users view scalability as a significant attribute that differentiates the wireless LAN vendors.

  Many companies are either using or planning to use wireless LANs to satisfy a variety of applications, such as the transmission of voice and video and other high-end functions. In most cases, these companies are not sure what applications they will need to support in the future. To fill the need for greater bandwidth and the uncertainty of future applications, there is a greater need for high capacity wireless LANs that offer synchronous transmission of time-bounded data. As a result, it is likely that companies utilizing 802.11b/g systems

today will need to scale up their networks through collocated access points or migrate to 802.11a or 802.11n systems in the relatively near future. As a result, consider incorporating load-balancing functions to maximize efficiency of collocated access points.

- Enhanced Quality of Service (QoS)

  The proliferation of voice and video applications has led to finalization of various QoS mechanism. For example, the IEEE 802.11 Task Group E finished the development of the 802.11e standard in 2005, which enhances the distributed coordination function (DCF) and point coordination function (PCF) of the 802.11 medium access control (MAC) layer. A new coordination function, the hybrid coordination function (HCF) includes the HCF Controlled Channel Access (HCCA) and Enhanced Distributed Channel Access (EDCA). These mechanisms allow the assignment of service classes to various types of traffic. For example, email could be given a lower priority service class as compared to voice. Most access points implement the EDCA protocol. Many wireless applications providers had developed proprietary QoS protocols prior to the release of 802.11e, and many of those vendors still sell products based on the proprietary mechanisms. The advantage of 802.11e over proprietary QoS, however, is that 802.11e enables interoperability among different client card and access point vendors. Consider the use of 802.11e for time-critical applications.

- Enhanced Security

  There is now widespread use of 802.1X port-based authentication using EAP-TLS and PEAP due to Windows support. Many companies are trying to migrate VPN-based wireless clients to using 802.1X to reduce costs. It's relatively expensive to scale VPN servers up to support the growing number of wireless clients. 802.1X offers a much less expensive approach. It's somewhat difficult to integrate 802.1X into applications, however.

- Distributed Antenna Systems (DAS)

  In many situations, companies need cellular and Wi-Fi connectivity for users inside facilities. A newer approach, by MobileAccess Networks, offers a creative, cost effective solution that combines both Wi-Fi and cellular signaling over the same infrastructure. Passive antennas throughout a building connect via coaxial cable to a centrally-located concentrator. Each antenna supports Wi-Fi and cellular frequencies.

  One or more access points connect to the concentrator, making it possible for companies to start with fewer access points for the same coverage area. For instance, one access point can support an area that would traditionally need four access points. As performance needs increase, the company can connect additional access points to the concentrator.

In addition to the lower initial investment, the passive antenna approach offers higher security and easier maintenance. With all of the active components (switches and access points) in a single locked room, it's much more difficult for a hacker to physically mess with the network. And, the installation and maintenance of the system is done in one place. Consider the use of a DAS for supporting wireless applications in newly deployed wireless networks inside large facilities.

- System Integrator Issues

  Most system integrators lack sufficient RF experience and training. This has led to the installation of wireless networks that don't fully support wireless applications, especially within enterprises. As a result, carefully evaluate existing wireless networks for supporting specific applications.