Wireless Design – A Birdseye View

Introduction:

The term "Wireless" is used very broadly and in various contexts - from cellular phones to portable TVs to portable digital assistants to in-premise VoIP (voice over IP) phones to automation products sensors and business data collection devices, etc. Each system's environment poses its own unique challenges of design; however, in many ways, basic project implementation considerations and design practices still apply. For the purposes of this document, the slant will be towards 802.11 wireless technologies.

Wireless design depends upon a variety of factors, some fairly obvious, some much less obvious. It's as simple and, at the same time, as complicated as one might imagine.

With early "Legacy" RF systems, UHF (licensed) and 900+MHZ SST (non-licensed), the answers were more straightforward. These systems were "proprietary" - the basic functionality of the systems was designed and controlled by the manufacturer of the product. Interoperability was a non-issue, because products had to be matched to a single brand or manufacturer. With these systems, each manufacturer's data protocol was proprietary and security was seldom an issue. Radio transceivers were fairly costly, so users were generally very conservative as to the number of units that were installed in an environment. Transmission distances were basically defined by the type of radio technology. It was a given that wireless surveys needed to be conducted because it was necessary to maximize placement of radios so as to provide optimum coverage patterns. Data transmission rates were limited, and so was the type of equipment that could utilize the technology. Typically, early systems in business and manufacturing environments limited use to Automated Data Collection (ADC) devices. These were often mobile RF data terminals that were either installed on forklift vehicles or carried as handheld units. Network infrastructures were in their infant stage, as were network cabling and power options. Wired network speeds were at or below the 10Mb range and wireless data rates were significantly lower. Fortunately, most data transactions for warehouse/distribution or manufacturing were very small and the bandwidth required was minimal. Cellular phones were just that – phones. There was no texting and definitely no web-surfing or TV broadcast viewing.

That Legacy technology, however, has evolved into a totally different product. It provides not only for open "open-systems" and "interoperability", but it also provides opportunity for a plethora of devices to connect to it. Bandwidth is significantly greater, cost is significantly lower, and the breadth of applications is up to the imagination – from simple ADC transactions to streaming video and multi-media presentations. Couple these components with the general ease of implementation – it doesn't necessarily take a rocket scientist to pull these systems together – and this leads many to believe that all products in this technology realm are equivalent and anyone can implement these systems.

While many off-the-shelf products may be readily available and simple for the SOHO (small office/home office) user to install, these systems are not designed nor meant for use in larger business enterprises. The Open Systems architecture model creates issues that must be addressed in a business environment. If a system is open, theoretically, everyone has access. That means that security is now a concern of much higher significance. It also means that if everyone has access to the technology, the technology may be everywhere. The business across the street may have similar technology in place. Where one or two

people might use the technology in a SOHO environment, multiply that by double and triple digits and you have the number of users a business environment may have. Current wireless data transmission rates are now in the broadband realm and devices that can make use of the technology range from the basic mobile device - such as those that have for many years been used in manufacturing and distribution environments - to PC workstations, notebooks, personal digital assistants and multi-media equipment.

Combine high user capacity with high device capacity, the diversity of devices, the scope of applications - and the system gets very complex very quickly. Basically, the current wireless environment is one of wide accessibility, convenience, and opportunity. In this context, the design of these networks needs to be approached with not only enthusiasm, but also with methodical and tactical care. With these thoughts in mind, the following are some guidelines that need to be considered in any wireless project.

Design Considerations:

As with any project, a good design begins with a good plan, and, a good plan has to take into consideration the project's purpose. In the initial stages, the design doesn't need to delve into the utmost granular detail, but in today's wireless environment, wireless can mean anything from in-facility data collection to global cellular networks. With a wireless project, initial considerations need to be given to the following:

- Purpose?
  - Meetings, Multi-media…..
  - "Instant" offices, sales personnel, visitors….
  - VoIP phones, In-Premise mobile phones…..
  - Plant floor manufacturing/distribution/data collection/work tracking….
  - Asset tracking, inventory management, materials disbursement……
  - Mobile Service/Route Accounting Support

- Environment?
  - SOHO (small office/home office)
  - Small Business (warehouse/business office/local area, etc….)
  - Campus/Hot Spots
  - Enterprise (multi-facility business, wide area, global network, etc…)
  - Industrial (Plant floor/manufacturing/mill yards, etc….)
  - Mobility (route accounting, maintenance checks, sales order entry, field service, etc…)

- Users?
  - One user, many users, local users, remote users….

- Application?
  - Software – custom, PC – or web-based…
  - Terminal emulation – host or mainframe….
  - Global network connectivity – road warriors, service personnel…

- Equipment/hardware required/who decides?
  - Team participation – IT, engineering, plant management, facility operations, users…
  - Wireless infrastructure hardware…
  - Wireless devices…
  - Network devices to support infrastructure…
  - Cabling/power…

- Network/Infrastructure Design?
  - Wireless Site survey/assessment…
  - Autonomous – vs. – Distributed management….
  - Security…

- Future Proofing?
  - Current technology…

Sustainable, Upgradeable….
Mainstream or edge….

- Responsibility, long-term/short-term?
  Project Manager….
  Consultant or Integrator…
  In-house personnel…

- Business Assessments?
  Budget…
  ROI….
  Sustainment costs (daily support/product upgrades/product repairs…)

- Implementation?
  Infrastructure Design Decisions…
  Security Parameters…
  Hardware/Devices (Network/User)…
  Procurement of hardware/software/service materials…
  Installation/Cabling/Power…
  Testing/Roll-out…
  Support/Maintenance…

Design Implementation:

Once the basic goals have been determined, organized implementation execution will do much to promote a project's success. In the current wireless environment, anyone may be able to implement a wireless solution, but not everyone has the skill set or expertise that comes with experience in this field. In an 802.11 environment, Access Points (or Wireless Routers), are the building blocks of an in-premise and often, point-to-point, wireless infrastructure. They are available from a variety of manufacturers and at a variety of price points. They may be SOHO (small office/home office), Enterprise (medium- to large-business), or Industrial (rugged for harsh environments) grade. They are available in several versions with variations as to data rates, throughput, bandwidth/channel availability and transmission range:

Typical Wireless Technology > (SOHO/Business/Plantfloor)	*900 MHZ SST (900-928MHz) (Proprietary)*	*802.11 b (2.4GHz) (Open)*	*802.11 g (2.4GHz) (Open)*	*802.11 a ?5/5.6/5.8G (Open)*	*802.11 n? (2.4/5GHz) (Open)*	*Bluetooth (2.4GHz)*
Licensed	no	no (ISM)	no (ISM)	no(ISM)*	no (ISM)	no (ISM)
Modulation Range (indoor)	~ 35 m	~ 38 m	~ 30 m	~ 35 m	~ 50+ m	~ 10 m
Data/Bit Rate (up to)	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	1-2 Mbps
Throughput (up to)	~ 192 Kbps	~ 5 Mbps	~ 22 Mbps	~ 27 Mbps	~ 108+ Mbps	~ .5 - 1M bps
Network Application	LAN/P2P	LAN/P2P	LAN/P2P	LAN/P2P	LAN/P2P	PAN
IP	yes/no	yes	yes	yes	yes	pseudo

ISM* - range in band generally available for any technology, some ranges may require licensing
no ** - In Europe, some bands may be unlicensed but restricted
n? - 802.11 n ratification is anticipated in early 2010
Reference: Specifications referenced from IEEE 802.11 Standards documentations
Stats focused on wireless data collection applications.

Figure 1

- Considerations for Wireless Implementation include -

- Wireless Survey/Assessment – personal or professional
- Infrastructure: LAN/WAN/PAN
- Access Points (AP): lightweight, autonomous, bridge, indoor/outdoor, antennas
- Devices: PCs, mobile PDTs, Ruggedized plant floor devices, Wireless VoIP phones
- Security: Encryption-vs.-association/authentication, Radius Server, Secure Shell
- Applications: Wireless monitoring tools
- AP configuration

Site Assessment/Survey: In today's wireless world, wireless signals abound everywhere and if one is going to implement a system, it's wise to first assess what impact the existing environment may have one the new system. The best way to do this is with a wireless survey/assessment. There are a variety of tools available for this type of assessment; however, all are not created equal. A basic wireless scanner tool may suffice for a home user, a small business office, or a relatively small (less than 30,000 square feet) warehouse; however, that same tool is not going to be the optimum choice for a larger business, warehouse, manufacturing or industrial environment, or an environment that is likely to have a reasonable amount of outside RF interference. Issues such as pre-existing RF signal, what type of signal, what strength of signal and what security is implemented, need to be considered and assessed. For the Enterprise or Industrial environment, more robust wireless assessment tools are needed, as well as the services of persons experienced in this field.

Infrastructure: Depending upon the size of the endeavor, a LAN (local area network), WAN (wide area network) or PAN (personal area network) are the most likely options for the network. And don't forget cabling and support appliances (switches, routers, etc.). Today's LAN/WAN technology speeds demand robust cabling and products capable of handling 100Mb to Gigabit data rates. A more localized PAN (small grouping of printers, or automation devices) would have less stringent requirements. Also to consider - are you building on an existing network or starting from the ground up.

Access Points – Choosing the infrastructure building blocks: APs designed for a home or small office user may function in a more demanding environment, but that is not their purpose and the differences in operations will be obvious as the demands of multiple users task the system. Similarly, APs designed for business or office environments may function in ruggedized environments, but they won't provide the degree of reliability that may be required in plant or manufacturing environments where even a fewl minutes of down-time can be costly. And, most important to remember, the Access Point (or Wireless Router) network must be homogeneous – mixing and matching of various vendor/manufacturers' products is a no-no. While the standards for the technology are "open", this only applies to the connectivity between the AP and the end device. It DOES NOT apply to the communications between the APs, either wirelessly, as bridge, or hard-wired on the network. If communication is not squeaky clean among the AP family, devices accessing the AP network will fare the worse.

Devices: This is by far the category that offers the most choices, from simply implementing a plant floor data collection solution with mobile/handheld data collection terminals to later adding on PC workstations for manufacturing stations that receive/transmit CAD drawings wirelessly. There may also be a request to add wireless access for conference/meeting rooms, VoIP phones or PDTs that feature multiple, combined

functionality – phone, data scanner, web-browser, in-premise and out-of-premise cellular connectivity. Generally, these devices play well together, but there is the possibility that transmissions from some may interfere with others. The best advice here is to first test any device before fully integrating it into the overall system.

Security: This is the category that can be the most critical, receives the most scrutiny (or doesn't) and presents the most complications. This topic is a paper of scope entirely to itself, but for general information purposes, the basics must be considered.

In techno-speak terms, aside from the very basic SSID (system identifier) code that is a central component of every 802.11 wireless system, wireless security essentially has two components – encryption (over the air security) and authentication (wired network access). While some early corporate users did implement additional network security protocols in their wireless systems, initial wireless technology implementations primarily relied on WEP encryption (wired equivalent privacy) as its over-the-air security.

WEP initially came in two versions – 64bit and 128bit. 128bit was recommended as the most secure, but various factors in the design scheme of this type of encryption rendered it out-dated and "unsecure" in a few years. Fortunately, the IEEE Standards for 802.11 provided for an additional layer of security by requiring a more secured response from the wired network, once the encrypted connection (association) was made.

This component of the IEEE suite of 802.11 specification is 802.1x. It incorporates both "encryption" and "authentication" as a security protocol. There is still an "encryption" key that allows the wireless "association" between a device and the Access Point. In addition, however, there is also an "authentication" portion that allows for a security "handshake/password" at a network level. In its most robust application, an additional server is required to validate (authenticate) an end user/device. The terms LEAP, PEAP, EAP and RADIUS server, all refer to authentication.

The newest 802.11x standard is WPA2 (Wi-Fi Protected Access2) and has superseded WEP and WPA as the security standard. It allows for both "personal" and "Enterprise" use. A SOHO user can set a PSK (pre-shared key) with an Access Point network and have a very strong security field. A business can implement "Enterprise" mode by using RADIUS server and utilizing EAP protocol options for a more robust security field.

WPA2 uses a high level encryption code (AES), and, also provides for a speedy hand-off of roaming devices within a wireless network. In a stationary (office where wireless notebooks basically "stay put") environment this isn't crucial; however, in an environment such as a warehouse or distribution center where users are constantly on the move, it is an important factor to consider.

Additionally, there are other options or levels of security that can be implemented, such as MAC filtering (subject to spoofing), VLAN segmentation, and even seriously secured "down-to-the-wired" network utilities that use a Secure Shell/Tunnel concept. But, the key really, is to give serious consideration to security and implement it.

Applications: What is actually running on the wireless devices, can dictate how many APs will be needed, how they should be configured and, to a degree where they should be located. It's critical to make sure

those responsible for assessing the environment and configuring the network understand what the network will be supporting. Small TE (terminal emulation) applications require very little bandwidth, while a user group in an office might require a medium portion of bandwidth and system-intensive processes like video-streaming or multi-media presentations very require a giant-size portion.

AP Configuration: Access Point products are primarily are in the 802.11 a/b/g range. (802.11n is on the horizon, and many vendors have been manufacturing equipment to this spec, but IEEE ratification of it as a standard is not anticipated before early 2010.) Each of these versions has its specific data bit rate and data throughput values. Both of these variables are a function of speed and wireless range (distance traveled). The higher throughput will be closest to the AP. As the radio waves propagate farther away from the APs, throughput drops. So, once it's understood what applications the network needs to support, the APs (typically, industrial/enterprise-grade models) can be configured and fine-tuned to provide optimum performance. But, please note that radio signal is a balance of strength and quality. "Coverage" is a component, but it has to be balanced with the available channels (dependent upon the radio specification in use) and the overall bandwidth.

Design Caveats:

Design caveats and misconceptions: less expensive access points are, well, less expensive but, they should work just as well as higher end models; standard, integrated antennas are sufficient; all antennas are the same; good cabling and installation practices don't matter, it's unnecessary to certify the cabling installation; it either works or it doesn't and if it doesn't, it must be the Access Points. And, probably the main caveat – the more APs, the better the coverage.

To address these more general misconceptions, it has to be understood that the SOHO environment is totally different from the business or enterprise environment. If a system fails in a home or small office, it is generally less disruptive than if a system fails in a larger business or on the plant floor. The costs of downtime in the latter can be significant. The key to a good wireless system design is to select the best of breed in terms of components and installation support for these systems.

This is not to suggest that the most expensive option is the best, but it does mean that it is crucial to consider not only price, but also factor in criteria such as quality, dependability, durability and reliable support. Short cuts in a system's design may save money upfront, but the long term consequences in terms of dollars and labor usually exceed any of those savings.

A system is only as reliable as its weakest link, so design the wireless system such that all components are configured, matched and tested to published system and regulatory standards. And, always follow recommended design practices when installing wireless systems. Today's Wireless systems have come a long way from the Legacy systems, and anyone can install them. However, avoid over-designing with too many APs. It's a common occurrence that creates its own issues.