Wireless LAN Network Management White Paper

A White Paper by:

90 East Halsey Road, Parsippany, New Jersey 07054 USA
Tel: 973-884-0100 · Fax: 973-884-8804
www.phillips-infotech.com

Table of Contents

WLAN Network Management

I. Overview

Until recently, acceptance of Wireless LAN (WLAN) networks has been slow due to many factors including but not limited to lack of standardization, slow data speeds and high costs. Recent market developments, however, have led to rapid market growth. The IEEE 802.11b standard, which was introduced in 1999, now enables wireless LANs to reach data rates up to 11 Mb/s. Demand for wireless LANs has also been fueled by growth in mobile computing devices such as laptops and personal digital assistants (PDAs), reduced prices and increased demand for Internet access anywhere/anytime.

Wireless LAN applications include Internet access, supply chain management and customer relationship management, to name a few. Traditionally, wireless LANs were used primarily in select vertical markets such as education, finance, healthcare, manufacturing, and retail. More recently, however, wireless LANs have appealed to enterprise customers and public access areas such as airports, convention centers and hotels. Wireless LANs are attractive to enterprise customers who manage large numbers of network adds, moves and changes for their transient employees, such as call centers, hot-desk environments for satellite offices and ad-hoc groupings of employees for meetings or training.

Even though wireless LAN networks introduce a new, flexible way of working, they present new challenges as well. Security management, data throughput maintenance, hardware interoperability and problem isolation can easily affect the overall satisfaction of wireless LAN customers. Moreover, network managers expect wireless LANs to have the same level of security, manageability and scalability as their wired LANs.

Faced with these new challenges, wireless LAN network management tools are now a requirement rather than a luxury for large, wired Ethernet-LANs; therefore, most wired networks have incorporated them. However, many of these tools do not adequately address the dynamic aspects associated with wireless networks and mobile computing environments. Wireless LAN network management tools have only recently reached acceptable levels. A wireless network management tool is a valuable solution for network managers deploying wireless networks because a wireless protocol analyzer, that can observe each of the layers of the stack, quickly reveals problems that other tools can easily miss. The short-term benefit of this tool is immediate reduction of the amount of time spent diagnosing or pinpointing whether the issue is wired or wireless in nature. The long-term benefit is that many of the network management tools provide immediate security and intrusion detection, such as identifying a rogue access point or transitive trust attacks.

While work still needs to be done to efficiently manage wireless LAN networks, there are a few vendors currently shipping network management tools which have gained significant momentum in usability, performance, interoperability and manageability. These vendors include Sniffer Technologies, Cisco Systems, Symbol Technologies, Lucent Technologies, WildPackets Inc., Wireless Valley Communications and 3Com.

II. WLAN Technology

Local Area Networks (LANs) offer the possibility for high-speed interconnection of fixed and movable terminals within a connected area. WLANs use radio propagation to provide LAN users with the flexibility of mobility by eliminating the need for a wire tether.

Background

Wired LANs use a physical medium to interconnect their terminals. Access nodes are provided at various points on the physical medium to allow for the connection of terminals to the medium. LANs may be interconnected by means of bridges or switches. The most common LAN protocol is Ethernet, with all of its evolutionary variations. The Ethernet protocol provides for message structuring rules, station naming, allocation of resources and other housekeeping functions.

Wireless LANs extend the access to a wired LAN's medium via an Access Point that attaches as a bridge to the wired LAN. The Access Point uses radio spectrum to extend the LAN's medium to radio equipped network devices within its radio range. Although many LAN protocols exist, and many wireless LANs can work with these other protocols, this paper will assume the use of the Ethernet protocol.

The most common WLAN configuration uses a single access point to provide service to all terminals within its radio coverage area. The Access Point is analogous to the base station employed in cellular networks and supports the shared usage of the spectrum by the active terminals. Specially designed access points are available to extend the LAN to an outside area surrounding the work site. Once associated with an access point, a terminal is a full-fledged member of the LAN, with all assigned LAN privileges. Wireless terminals may talk to each other, to other wireless terminals on the same or different access points and to devices on the wired LAN. Up to 100 terminals may share an Access Point, if individual terminal usage is low.

Terminals may roam among the multiple Access Points without losing their connection. However, if the access points are in separate subnetworks within the wired LAN, roaming may not be possible due to routing constraints within the LAN.

In addition to communication through a wired LAN, wireless terminals may also directly communicate with each other when they are within radio range. This is called a peer-to-peer or ad hoc network; this type of network does not require an Access Point.

Standards

A key to achieving system acceptance is device interoperability. Interoperability allows end-users to purchase parts from their preferred vendors and be assured that they will

work with each other, and with other vendors' equipment. To assure this, standards and conformance testing are necessary. Standards also permit the design of universal network management tools.

The IEEE 802.11 standard is emerging as the dominant physical and medium access control (MAC) sublayer standard for WLANs. The standard allowed for both direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) radio layers, and an infrared physical layer; all these technologies use a common MAC layer. This 1997 standard supported rates of 1 or 2 Mb/s, with the system automatically selecting the highest usable rate. In 1999, higher speed versions of the standard, referred to as 802.11b and 802.11a, were adopted.

The Wireless Ethernet Compatibility Alliance (WECA) is a nonprofit organization that certifies the interoperability of wireless LAN products. When wireless LAN products successfully pass WECA's interoperability tests, conducted by an independent testing lab, they will be granted the Wi-Fi seal of interoperability (www.wirelessethernet.com).

Spectrum

Governmental regulations authorize use of specific radio frequencies and transmission parameters for each radio application. The most common WLANs operate in the unlicensed 2.4 GHz ISM (Industrial, Scientific and Medical) and the 5 GHz UNII (Unlicensed National Information Infrastructure) frequency bands.

IEEE 802.11b WLANs use DSSS modulation and operate in the 2.4 GHz to 2.4835 GHz range in most of the world. (Narrower allocations are authorized in France, Spain and Japan.) Eleven sub-bands are defined within this range in order to permit several WLANs to operate in the same area. To achieve minimum interference operation, only three of these bands should be used in the same area. DSSS systems are authorized to use up to 1 Watt of radiated power, but most systems operate at 30 milliWatts (mW), or less. This reduces range but conserves battery power.

IEEE 802.11a WLANs use the 5 GHz UNII band. This band is 300 MHz wide and is split into two blocks. The lower block extends from 5.15 MHz to 5.35 MHz. The upper block is from 5.725 MHz to 5.825 MHz. Power is restricted to 50 mW in the first 100 MHz, 250 mW in the middle 100 MHz and 1 Watt in the highest range. While benefiting from the broader bandwidth available at 5 GHz, IEEE 802.11a products have poorer propagation and more complicated equipment designs.

The entire UNII band is reserved in the United States. The Japanese have only allocated the lowest 100 MHz of spectrum, and in Europe, only the lower 200 MHz band is available for WLANs. Furthermore, ETSI's (European Telecommunications Standards Institute) HiperLAN2 uses this same spectrum.

802.11b

The original 802.11 standard provided too low a data throughput at too high a price to be widely adopted. In 1999, the IEEE 802.11 committee issued a new standard, 802.11b, that supports basic data rates up to 11 Mb/s. When radio communication is poor, the system can fall back to rates of 5.5 Mb/s, 2 Mb/s or 1 Mb/s in order to maintain connectivity. 802.11b is backward compatible with the original 802.11 standard, but it is

only defined for a DSSS physical layer. Because of the backward compatibility, users can easily migrate from the older standard to the new standard.

Most 802.11 products will work indoors and achieve a range up to about 500 feet under optimal conditions. (Special antennae are available for extending this range for an essentially open area or point-to-point transmission.) However, many customers are using a 100-foot rule-of-thumb to assure good performance without having to do extensive engineering studies. As the radio signal deteriorates, the systems will back off to the slower rates.

IEEE 802.11 provides for authentication and encryption. Authentication may be based on a user-defined list or a shared key. Not all manufacturers, and not all of the products from the same manufacturer, support the same levels of security. The IEEE 802.11b standard only mandates a minimal level and defines more secure levels as options; however, Wi-Fi certification requires products to support at least a 40-bit Wired Equivalent Privacy (WEP) encryption key.

The WEP encryption option is available with most manufacturers' wireless LANs, but not necessarily in their complete product line. Only the data transmitted is encrypted. Headers are broadcast in the clear.

Additional information can be obtained at the IEEE web site (http://standards.ieee.org) or from the Wireless LAN Association, WLANA (www.wlana.com).

802.11a

The IEEE ratified the 802.11a standard in 1999 recognizing that video and intensive multimedia applications would require data rates higher than 11 Mb/s. The 802.11a standard is optimized for high performance in indoor environments. It specifies methods to be used for transmitting data rates of up to 54 Mb/s. One manufacturer has even claimed to be able to go beyond the standard with a proprietary approach that supports a rate of 108 Mb/s.

IEEE 802.11b uses the full bandwidth of each subchannel to modulate its signals. IEEE 802.11a uses a different approach called Coded Orthogonal Frequency Division Multiplexing (CODFM). The lower 200 MHz are subdivided into eight channels of 20 MHz each. (The additional 40 MHz is for channel separation.) Each channel is subdivided into 52 subchannels, each approximately 300 KHz wide. These narrower channels improve data transfer because they are less subject to time and frequency dispersion. Of the 52 channels, 48 are used for data and the remaining four are used for error detection.

Each channel uses phase shift keying. The standard requires compliant systems to support binary and 4-, 16- level quadrature modulation for each channel. These correspond to rates of 6, 12, and 24 Mb/s respectively. 802.11a also specifies higher coding rates corresponding to data rates of 36, 48 and 54 Mb/s.

802.11a and 802.11b technologies should be able to operate on the same LAN since they use the same MAC and operate on different frequency bands. However, the differences in propagation may make it necessary to re-engineer the radio coverage.

Further discussion of wireless LAN standards is presented in the Appendix, Section V. The standards described are for extensions to 802.11 that increase the security of the 802 standards and the standards for Bluetooth and HomeRF. These two standards are for wireless voice and data terminals and are optimized for a narrower set of applications than the 802.11 standards.

III. WLAN Applications

There are a variety of applications for WLANs. These products meet the same customer needs as wired LANs (except with a lower maximum data rate) and solve the same business problems; however, the mobility and flexibility inherent in WLANs allow them to support additional applications. The most important application categories include:

1. Universities, IT professionals or business executives who want mobility within the premise, frequently in addition to a traditional wired network.
2. Business owners or IT directors who need flexibility for frequent LAN wiring changes either throughout the site or in selective areas.
3. Vertical businesses that connect data from a variety of places or that regularly modify the size of their work force.
4. Any company whose site is not conducive to LAN wiring because of building or budget limitations, such as older buildings, leased space, or temporary sites.
5. Business groups that frequently use temporary or contract employees and need to provide them with Internet access, or access to each other.
6. Travelers who need access to e-mail and the Internet while on the road.
7. Travelers who collect data while on the road and need to synchronize with Enterprise data while back in the office.
8. Home and small business owners who have a need to share access across a group of users.
9. Organizations, such as standards bodies, that assemble for short periods in public spaces, e.g., in hotel meeting rooms.

Recent market extensions have expanded the appeal of wireless LANs to new types of customers such as universities and homes. In addition to private WLAN installations, several service providers are providing WLAN access in public places, e.g., airports, restaurants and hotels which extends the availability of e-mail and corporate databases.

Benefits

In a recent study by InfoTech, the most frequently cited benefits of WLANs were identified as:

1. A user is always connected, with no wires and full mobility – enjoying the capability and functionality of Ethernet – used as an Ethernet substitute or

extension to a wired Ethernet or other LAN. This application avoids the mess of dongles and wired links to the hubs.

2. Users are able to do anything they can do with a fixed network: send and receive e-mail, retrieve and send documents, access corporate data and applications, and connect to the corporate intranet – a laptop computer is automatically connected to the network when it is turned on within the WLAN coverage area.
3. Users can roam seamlessly within a site and roam from site-to-site and stay connected.
4. WLANs open up new ways of working: for working in groups, for off-site teams and for mobile workers.
5. WLANs provide users with wire-free, untethered connectivity in the classroom, the boardroom, the library, the cafeteria, the campus, etc.
6. WLANs make "hot desking" and "hoteling" more effective as Enterprises use common office areas for multiple employees who only are in the office on a part-time or occasional basis.
7. Organizations also are using WLANs to introduce enhanced working environments, providing users with the ability to work anywhere on the site or campus, both inside and outside of the buildings, and provide maximum flexibility in the ways that staff work, individually and in teams.

Problems

In the same study by InfoTech, potential and current users were each asked to rate their problems with WLANs.

As seen by non-users

- Lack of awareness
- Inadequate reliability
- No compelling application
- Inadequate security
- High cost
- Lack of budget
- Confused standards

As seen by users

- Dead spots in the coverage
- Costs of equipping a large user population
- Inadequate throughput

- Limited interoperability
- Lack of voice capability

Good network management tools can address many of these user issues, e.g., reliability, security, RF coverage, optimal throughput, and operations costs.

Examples

Below are three examples of wireless LAN applications and how network management tools can solve some of the wireless LAN problems encountered by these installations.

- *University of North Carolina*

  Many universities require incoming students to have computers, and more and more of these schools are requiring that these computers be equipped with wireless modems. Carnegie Mellon was one of the early adopters of wireless technology. Examples of more recent conversions are Princeton University and the University of North Carolina (UNC). In addition to equipping students, wireless computers have also been made available to the faculty.

  UNC students are using wireless technology for access to the Internet, e-mail and the campus network in classroom, laboratories, libraries and other nearby sites. All 3,400 freshmen have been required to own laptop computers. Access points have been installed at 40 locations. By 2003, when the current freshmen are seniors, wireless laptops will be in use by 15,000 plus students.

  Carefully placed antennae at one edge of the campus also extend UNC's wireless radio signals to nearby businesses, including Café Trio, a coffee shop, and Hector's, a fast-food restaurant. The Chancellor's residence is also covered, allowing the Chancellor to work from his university-owned residence.

  UNC believes that wireless will increase flexibility in classrooms but will also extend the learning experience to the campus' green spaces and coffee shops. WLANs were installed even though an extensive wired network already existed in all of the residence halls. Wireless has allowed the LAN to be accessible in older buildings that could not easily be wired, as well as in the outdoor and social areas of the community.

  An obvious benefit to the network manager is the ability for students to move around this entire complex without requiring them to locate physical hubs or change access parameters. The problems this university faces that can be resolve with network management tools include: assuring that enough capacity is available to support the dynamic movement of terminals, identifying the best places to install new Access Ports, identifying low throughput locations and assuring that only authorized terminals are accessing the network.

- *Medical Application*

  A large medical complex is exploring the potential of using WLANs to change their method of managing data and interacting with patients. Their initial exposure to WLANs occurred when they equipped six operating rooms with WLANs. Technicians needed to be able to briefly enter the operating room and transfer data from laptops to equipment within the room without having to manually connect to the existing LAN, which would have been difficult to extend into the operating rooms due to ceiling problems. Before installing the application, the hospital carefully examined the issues of user authentication and RF interference with medical equipment; IEEE 802.11 equipment met both of these tests and has been successfully employed.

  In its next phase, the hospital would like to use wireless to fundamentally change the way it operates. They would like hospital data management functions to follow the personnel, rather than making the personnel run around the hospital to find the location providing the service. Data could also be made more easily available to specialists within the hospital. Some of their intended applications will require bandwidth of up to 8 Mb/s. Wireless supports the intended application well because it allows personnel to carry laptops and other portable terminals to the patient for data gathering and, in this case, it could be less expensive than cable.

  Because of the critical nature of their application, the hospital requires network management tools that allow them to rapidly identify and respond to problems using their internal resources. Enforcing the implementation of authentication and encryption features is critical because of recent federal regulations (Health Insurance Portability and Accountability Act) that have drastically increased hospitals' requirements to protect the privacy of patient information. The hospital is also looking for the ability to manage quality of service and to have independent virtual LANs share the same access points because of the need to support multiple applications

- *MobileStar Network*

  As the explosive growth of cordless and cellular telephony has shown, people attach significant value to mobility. Much attention has been focused on new 3G cellular technologies to provide mobile data access. Several service providers have already entered this market with IEEE 802.11b WLAN support for mobile people using laptops. In mid-1999, MobileStar Network (MN) launched a nationwide service enabling wireless broadband access at participating facilities, called Public Access Locations (PALs), to business travelers. Subscribers with laptops or Windows CE-based devices are able to wirelessly access the MN network for 1 Mb/s broadband connections to the Internet. Initially MN contracted with American Airlines and its Admirals Clubs. Since then select Hilton, Sheraton, Holiday INN Select and Crowne Plaza sites, and other hotels and airports have also agreed to integrate the MN network with their facilities. Recently MN has added Starbucks to their list of service sites. Moreover, AdAlive has announced a service that uses MN's

airport network, with specialized terminals, to allow travelers to download local information into their PDAs as they pass through airports. There are several other service providers, such as Wayport, in the public access wireless LAN market.

Key success factors for MobileStar Network are the ability to rapidly resolve customer performance problems, to support a thin-network distributed over the entire nation and to accurately identify subscribers to support billing.

IV. Management Tools

Early WLANs were small, making it relatively easy to rely on manually operating the network and managing radio coverage by trial and error. Users would detect failures and report them, interferers were few and hackers had not yet found WLANs interesting. Manufacturers could closely support their products. This has changed as the number of installations has grown, networks have become larger and their uses have become more critical to the Enterprise. In addition, network mangers are reluctant to deploy wireless LANs unless they provide the same level of security, manageability, and scalability as their wired LANs. Network management and network management tools are critical throughout the lifetime of a WLAN; the life cycle stages span development, deployment and operation.

IEEE 802.11b network management tools are no longer a luxury for large Ethernet LANs that incorporate wireless capabilities. They are needed to control network-operating costs, to locate the causes of network problems and to spot security risks. Tools have been incorporated into these Ethernet networks that support the operation phase of wireless network management. However, they are of minimal use for development and deployment. In addition, many of the integrated tools do not adequately address the dynamic nature of the wireless environment. Traffic demands and radio performance change dynamically and network performance as seen by users can suffer if the network parameters are not optimized and reviewed regularly. Long-term throughput degradation resulting from poor performance can be even more costly to an Enterprise than short-term total outages. Correction may involve redesign of the radio transmission plan as hot spots are discovered, as interferers move into the area or as new coverage areas are required. In order to get all of the performance that the Enterprise expects from the WLAN, procedures and tools must be in place to regularly monitor performance and allow the network manager to easily identify the root cause of the performance problem.

Development

During the development stage, the designer needs to be able to verify that the equipment is compliant with the standard and operating properly. A critical tool at this point is a protocol analyzer that can check all of the required operations and easily identify the underlying problem when the product is not working. Mobile network management products are of great value in this phase. They can be used to monitor performance on each of the available radio channels, verify throughput and performance under various conditions, prove the ability to correctly encrypt data, separate MAC problems from

higher layer network problems and check that all design features are operating in accordance with the specification.

Deployment

While WLANs can be thought of as extensions to an existing wired LAN, their deployment adds complexity. All of the problems associated with deploying a large wired network come into play. In addition, the problems created by mobility, security and radio link performance must also be considered. Network architects and managers must consider:

- How to locate Access Points in order to have a cost-effective WLAN with adequate coverage
- How to optimize network performance and availability in the uncontrolled wireless environment
- How to verify that all of the piece parts in the total (wired & wireless) network work together

Mobile network management tools can be used during this phase to identify areas of inadequate radio coverage before the network is made available to users. Sites subject to radio interference can be identified and the Access Points can be tested to insure that the proper parameters have been installed. As terminals are added, customer problems can be easily isolated into those caused by MAC layer problems and those due to protocol or parameter mismatches at the higher layers. Network routing problems can also be identified before they cause customer complaints; these problems can be isolated and the root causes identified and fixed.

Operation

Once a WLAN is up and running, it needs to be operated just like any other LAN. The operator needs to be able to add and configure new equipment, optimize the performance and identify, isolate and repair network problems. Most WLAN vendors provide an integrated capability to manage the products that they provide. For WLANs, significant differences exist among the management capabilities available from different manufacturers, and even among different generations of equipment from the same manufacturer. There are as yet no standards and the equipment capabilities are evolving rapidly. In addition to the integrated facilities, portable network management tolls can help in responding to user problems accessing the network.

The following paragraphs identify some of the unique elements that must be administered by the operator of a WLAN.

Access Point Administration

Access Points are the devices that tie the radio system into the wired LAN, providing access to the LAN for the wireless terminals. Access Points are a bridge that connects

multiple terminals to the network and provides the means for managing those subnetworks.

The Access Point is a complex network element. Some of the WLAN features that might be managed in the Access Point are:

- Device IP address and subnetwork mask for the LAN (if directly attached to a LAN)
- Service Set ID (SSID) to identify the network
- Radio parameters, e.g., power, assigned RF channel(s), conditions for handing-off terminals to adjacent access points, multicast rate, data beacon rate, radio transmit power, …
- IP address of the default Internet gateway
- System name to be used in addition to the device MAC
- Ethernet interface parameters, e.g., connection speed & duplex mode, DNS IP address(es)
- Traffic control parameters, e.g., protocol overhead messages to be filtered, packet life limits, preamble length, maximum message rate thresholds, RTS/CTS (Request-To-Send/Clear-To-Send) thresholds, …
- Security parameters, e.g., access control lists, access encryption method, terminal authentication process, RADIUS server identification, encryption keys, MAC address filters, fragmentation thresholds, …
- SNMP parameters of the access point itself, e.g., read/write passwords, SNMP traps, trap host identification, access point identification and location, software release, …

Each of these must be entered and maintained for each access point on the network. Some are necessary to define the physical system and others can be set to optimize performance. Where more than one radio is deployed in an access point, each radio must be individually configured.

Terminal Administration

Each wireless terminal must be configured for access to the network. The administered data that might be assigned includes:

- One or more wireless network names, e.g., SSID
- IP address(es) of the preferred Access Points
- Client name used to identify the client to the network administrator in addition to the MAC address
- Power save parameters, e.g., wake duration
- Encryption keys and encryption mode, e.g.. None, WEP keys

- RF power parameters and the threshold that triggers a transfer between access points
- Maximum data rate
- Data retries and fragmentation threshold
- Permission to engage in peer-to-peer communications
- Authentication mode, possibly including user ID & password or EAP[1]
- Software, firmware & hardware version information

Security

By their very nature, wireless signals are easier to intercept than wired signals. It is not necessary to have physical access or even to be within the same physical room to monitor the communications channel. IEEE 802.11b defines many levels of security that may be implemented. The network administrator must be able to assign the appropriate security permissions and verify that they are being implemented. The security features available in 802.11b include:

- Authentication – Terminals which do not know the network name, or which are not on the list of recognized terminals can be denied access to the network. The PC card's MAC can be used to identify authorized stations. Use of encryption for authentication can be specified. A RADIUS server may also be included in the system to support network login with password protection for authentication. The RADIUS server must be administered to manage the lifetime of access passwords and user IDs.
- Data Encryption – IEEE 802.11b provides for both 40- and 128-bit encryption of the transmitted data. (While most manufacturers support 128-bit WEP, administration of these keys may be manufacturer specific.) Key sizes cannot be mixed within a network. Access points can be set to deny access to unencrypted traffic. To simplify management of the encryption keys, systems can be configured to recognize more than one key. Thus, during key transition periods, both the old and the new key will be valid. Equivalent keys must be set in both the Access Point and the terminal. Since wireless terminals can be easily lost or stolen, keys must be changed more frequently than would be the case on a wired network. Optionally, the network's multicast and broadcast traffic may also be encrypted.
- Privacy - Adding wireless capability to a wired LAN, without enforcing security measures is equivalent to adding public network access to the wired LAN. The access points may be broadcasting information that is company confidential, e.g., they may be inviting hackers by broadcasting in the clear an SSID that identifies the Access Point as belonging to the "payroll" network subsegment. Security measures must be established and enforced because others can easily eavesdrop on the wireless signals.

[1] Extensible Authentication Protocol

- Access Points may be configured to limit access for administration to specific administrative terminals, with or without password protection.

Monitoring

A wired LAN's performance is relatively constant once the configuration has been established. The performance of WLANs will vary with time because of changes in the radio environment and the transient nature of the terminal connections. Therefore it is necessary to regularly monitor the performance of the wireless segments of a network. Some of the items that should be monitored are:

- Signal and noise levels – These may indicate the presence of competing networks or radio noise generators, e.g., microwave ovens. Monitoring devices are required to identify these noise sources, some of which could be time dependent. Dead spots in radio coverage may also occur because of furniture or office partition relocation.
- Transmission rates – In noisy or low signal environments, the LAN may appear to function, but at reduced transmission rates of 5.5-, 2-, or even 1-Mb/s. Low transmission rates may indicate a need to modify the network configuration or parameters.
- Throughput – Low throughput may indicate frequent packet retransmission caused by excessive traffic, transmission of unnecessary overhead packets or hidden terminals. The presence of hidden terminals may require changing the terminal access protocols to one in which the access point controls admittance to the network.
- Security feature implementation –Security verification is important in wireless networks for the same reason that it is in wired networks. New out-of-the-box equipment is normally shipped with all of the security features disabled and, unless administered, will permit breaches in the system. Also, since wireless devices are inherently mobile, users will prefer to have minimum terminal security so they can attach themselves to public networks where they are available.
- Access Points – It is necessary to be able to find rogue access points added by clients and to verify the actual location of installed Access Points.

Network Management Products

While great strides have been made in assuring interoperability of IEEE 802.11b products, the same could not be said about the network management tools until recently. The standards do not specify diagnostic or management tools. As recently as July 2000, a Network Computing magazine article described them as "pathetic." Recently announced products by the major WLAN and management tool vendors have greatly improved the situation. The following paragraphs briefly describe some of the newer management products.

Network management products tend to fall into two categories: stand-alone portable terminals that can act as protocol and packet analyzers, and integrated systems that can manage network and terminal parameters and collect information as seen by the network or Access Point.

The mobile terminals can be used in the development and deployment phases, as well as the operational phase; they can more readily identify external interference or attacks and isolate problems between the wireless and wired environments. Some can analyze all of the protocol layers, including those protected by encryption, in order to immediately diagnose errors caused by parameter mismatches.

The integrated systems support the operation stage of the system, allowing for centralized equipment management and monitoring; they can observe the performance of active terminals, as seen by the Access Point. However, integrated systems have limited capabilities for trouble shooting since they can only "see" what the Access Points report, and they cannot monitor what the Access Points broadcast, terminals that are having difficulty accessing the system or external sources of radio interference. Integrated systems are of minimal use in the development or deployment phases, where a protocol analyzer and a radio monitor can reveal and isolate problems that these other tools miss.

The following paragraphs briefly describe some of the available network management tools.

Sniffer Technologies

Sniffer Technologies is a Network Associates business that provides a variety of products for monitoring, troubleshooting, performance reporting and proactively managing LANs, WANs and WLANs. Sniffer's wired LAN product, Sniffer PRO, analyzes network traffic and incorporates "expert" analysis to highlight the likely cause of the problem.

Sniffer's WLAN product, Sniffer Wireless, complements their wired LAN capability. A recent eWeek magazine review of Sniffer Wireless reported that it collects more data and with less effort than other tools available. Sniffer Wireless is a portable device that is being used in the development, deployment, operation and monitoring of WLANs.

In its monitoring mode, Sniffer Wireless displays a "dashboard" showing all of the important IEEE 802.11b statistics, including an overview of how many packets are sent at each of the permitted speeds. Data on the Access Point's overhead transmissions ensure that unnecessary information is not being transmitted and wasting spectrum. Statistical details can also be accumulated for each active terminal. While in the monitor mode, it places a minimal burden on the radio network. To assist in locating transient problems, the Sniffer product can be set to collect statistics at a pre-selected time, do data collection over specified periods, or in response to observed triggers.

Sniffer Wireless can scan all of the designated IEEE 802.11b channels, identifying transmitters that are broadcasting in its area. It can also monitor the level of signal and noise from nearby access points. These may be part of a neighboring network and creating interference that reduces network performance. Interferers cannot be readily identified any other way. This monitoring capability can also be used to verify that

Access Points are installed where the network designer anticipated and that the desired coverage area has been achieved. This can all be displayed in one view.

Sniffer Wireless can monitor to insure that security practices are being enforced, i.e., unencrypted traffic is not being allowed onto the network or that users with the default network identification of "any" are being denied. This capability also will detect intruders attempting to log on to the network.

To help in isolating LAN configuration problems, Sniffer Wireless can look at all layers of the communications protocol, from physical to application. This includes the ability to decrypt the WEP encoded data, and observe each protocol layer up to the application layer. Individual packets can be observed and retransmissions identified. This makes it possible to quickly identify configuration problems occurring due to protocol mismatches at any of the protocol layers.

Once data is collected, Sniffer's "expert analysis" capabilities automatically provide the network manager with specific recommendations about the probable problems and their causes.

Sniffer Wireless is basically a software application included in a laptop equipped with an IEEE 802.11b card. Cards from different manufacturers will interoperate, but since some of the administrative and security messages are manufacturer-specific, the tool must be tuned for each product. Sniffer Technologies has already announced specific interfaces to work with Cisco Systems (Series 340) and Symbol Technologies (Spectrum24®) WLAN cards. Other interfaces are planned, including one with Agere Systems' (formerly Lucent) ORiNOCO products.

Additional information on their products can be obtained at www.nai.com.

Cisco Systems

Cisco provides an extensive line of LAN equipment, and their recent acquisition of Aironet has given them a significant presence in the WLAN market. Cisco recently announced their Cisco Aironet 350 Series, which addresses the market for large WLAN installations. This product line includes access points, terminal cards, bridges and administrative tools. Operation support for these networks will be provided as part of their CiscoWorks family of products. CiscoWorks is an integrated network management product. Use of Cisco Delivery Protocol enables auto-discovery of the wireless infrastructure. BootP and DHCP are supported with appropriate access point configurations.

The security features for this new product include RADIUS server support in anticipation of the IEEE 802.1x standard. This has been incorporated into the Cisco Secure Access Control Server. This provides for user level authentication and automatic generation of single session, single user keys. This eliminates most of the problems associated with key management.

The RF frequency utilized by each access point is adjusted dynamically to improve performance. Broadcast and multicast filtering is supported. Use of collocated backup access points for reliability, sharing the same RF channel as the active access point, is also supported.

CiscoWorks will be able to collect data from each Access Point in order to determine the throughput performance of each active terminal. Data can be collected on signal strength, in-band noise levels, error rates, transmission speeds and other performance variables. These data can be used to infer the condition of the radio links and terminals attached to the network. Statistics can be collected at specified times or in response to recognized triggers.

Additional information can be obtained at www.cisco.com

Symbol Technologies

Symbol Technologies provides a wide range of WLAN products. These products range from networks optimized for real time data collection e.g., wireless barcode scanners, to general purpose LANs.

Symbol's most recent entry into WLAN network management tools is their SpectrumSoft Wireless Network Management System (WNMS). WNMS is an integrated network management system that provides a migration and expansion path from single site management to multi-site management and eventually to completely integrated Enterprise management systems such as Open View, Tivoli and Unicenter.

WNMS is optimized to work with Symbol's Spectrum24 wireless networks, and it allows configuration setting for access points and terminals. New access points can be automatically discovered. WNMS supports data trending to track network traffic and usage with proactive analysis of network utilization. The software enables exception based management by distributing event driven data collection and threshold analysis into the enterprise system.

Additional information can be obtained at www.symbol.com.

Agere Systems[2]

Agere Systems offers a network management software suite as part of its ORiNOCO product line. These tools can run on a variety of Windows platforms and enable the user to

- Display and modify the configuration of network components
- Configure the network components
- Manage and optimize network performance
- Monitor the performance of transmission over the radio links.

The tools allow for local or centralized setting of all of the necessary network parameters. ORiNOCO Access Point Manager supports centralized monitoring of the network. It can collect the SNMP data and packet transmission statistics that are collected at each access point. It can also collect radio measurements for the link between an access point and one of its active terminals.

[2] Agere Systems was formerly the Microelectronics Group of Lucent Technologies. Because of the various Lucent divestitures, nearly identical products with differing names are available from Agere and Avaya.

A portable unit, using ORiNOCO Client Manager, allows for observing the name of the associated network (SSID), the quality of the network connection, and the name of the connected access point, the channel being used and the status of encryption on the link. It is also possible to identify other access points that can be heard in the area. Similar data may be collected on a peer-to-peer basis with another terminal.

Additional information can be obtained at www.orinocowireless.com.

WildPackets Inc.

Wildpackets, like Sniffer Technologies, is primarily a vendor of network management equipment. Their LAN management product is EtherPeek. Last year, EtherPeek was augmented to analyze Cisco's Aironet 340 WLAN products. WildPackets recently announced the release of their AiroPeek product. This product supports all higher-level network protocols such as TCP/IP, AppleTalk, NetBEUI and IPX.

In addition to EtherPeek's feature set, AiroPeek will isolate security problems, fully decode 802.11b WLAN protocols, and analyze wireless network performance to identify signal strength, channel and data rates.

Wildpacket has announced AiroPeek support for Cisco Systems' Aironet 340 series products and will soon add support for other wireless NIC cards including those from Symbol Technologies and Agere Systems. The AiroPeek requires installation of a special NDIS driver supplied with the software.

Additional information can be obtained at www.wildpackets.com.

Wireless Valley Communications

Wireless Valley Communications, Inc. was founded in 1995 and is a leading provider of in-building wireless system design, measurement, maintenance, and asset management products. Wireless Valley develops products that allow engineers and facilities managers to design, deploy, and maintain every type of indoor wireless network, including Cellular/PCS/Wireless LAN/Bluetooth, and emerging LMDS and optical systems. Wireless Valley's products help to predict the optimum locations for RF transmitters in order to assure good coverage throughout a site.

Wireless Valley's LANFielder™ product provides real-time, site-specific network performance measurements for any IP-based data network, including 802.11. It measures throughput, delay and packet errors. Summary statistics include detailed packet counts by RF channel and terminal throughput. Both of these are available plotted versus the time of day. Results are displayed on a 3-D model of the operating environment.

Additional information can be obtained at www.wirelessvalley.com.

3Com

3Com recently announced a new wireless strategy that focuses on reliable performance, mobility, security, and management. Since end user needs for security vary across organizations, 3Com offers customers a layered approach to security, allowing customers to select the best solution for their network environment. 3Com already supports 40-bit

shared key WEP. In addition to WEP, 3Com also supports more robust layer 3 Virtual Private Network (VPN) solutions (IPSec or PPTP) for larger organizations that rely on RADIUS-based authentication and authorization. For smaller sites that do not use RADIUS, 3Com supports an alternate VPN approach with its 128-bit Dynamic Session Key security.

3Com announced that they plan to incorporate the new IEEE 802.1x authentication standard in their wireless LAN platforms for enterprise, small business and public access. The technique, which is a key feature in Microsoft's new Windows XP operating system, provides a "network login" capability between PCs and edge networking infrastructure. 3Com will ship 802.1x in its line of business and public access wireless LAN solutions once the final standard is approved by the IEEE in the 2nd half of 2001.

Additional information can be obtained at www.3com.com.

Management Examples

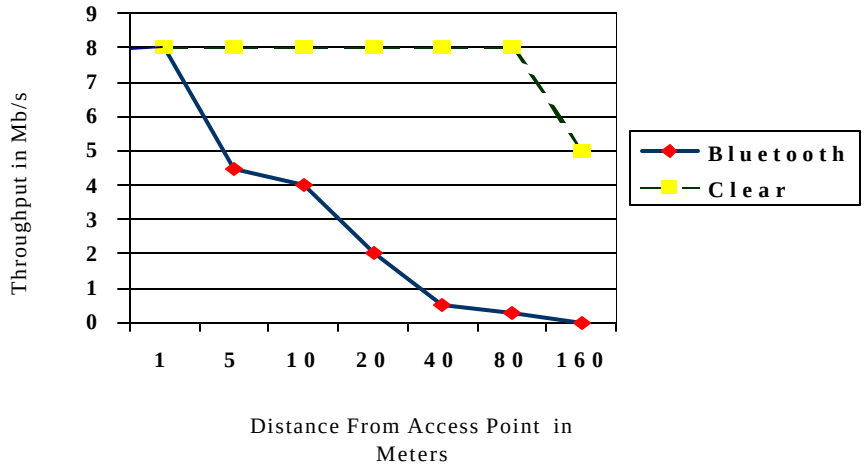
Development Tools

ShareWave is a key component supplier for the wireless home network market. While developing their products for the IEEE 802.11b market they needed a product that would allow them to validate their designs in terms of conformance to the standards and performance under a variety of operating conditions. ShareWave used the Sniffer Wireless tool as a protocol analyzer throughout the course of their development. Within the laboratory they were able to validate their designs and test all aspects of the protocol. Because of the detail of data that could be collected, the cause of troubles could be rapidly identified. A WEP implementation problem was quickly detected and corrected in this way. The protocol analyzer capability made it possible to distinguish errors caused by internal bugs from interoperability problems with equipment from other vendors

After the basic design was solidified, ShareWave's equipment could be taken from the laboratory and tested in a variety of field conditions to insure that it operated as expected. The portability of the Sniffer Wireless equipment made test setup rapid and unobtrusive. The equipment could be tested under a variety of real world transmission and interference situations. The Sniffer Wireless tool also greatly reduced time to market.

Interference

An important parameter of any LAN is the data transmission rate. With an 11Mb/s channel between the terminal and the access point, IEEE 802.11b can sustain a data transfer rate of about 8 Mb/s under good radio conditions. The difference is due to overhead in the protocol, radio handshaking, operating system and driver inefficiencies and other factors. This data rate can fall even lower if the station is shielded from the access point or an interfering network operates in the same neighborhood. The following illustration of this effect is based upon data published in Network Magazine. Data throughput is plotted as a function of distance from the access point under good conditions and with an active Bluetooth piconet in the vicinity. Network management tools must rapidly detect the inadequate performance and provide enough local data to enable the network manager to resolve and correct the problem.



Similar interference effects can be seen if HomeRF, uncoordinated 802.11b systems or even microwave ovens are operated in the immediate vicinity of an Access Point.

Performance can also be degraded if two terminals can "see" the same Access Point but cannot "see" each other. Transmissions could collide with each other at the Access Point unless the Access Point is configured to allow it to take control and tell terminals when it is permissible for them to transmit.

Future

It is clear that IEEE 802.11b has achieved a high level of user acceptance. It works as predicted and products from multiple vendors do interoperate. The remaining problems are not application killers. Throughputs are high enough to satisfy most applications, although there is only limited capacity for voice services. (InfoTech's recent study indicated that a voice capability would convince many non-adopters to seriously consider WLANs.) Short term, additional access points, each serving a smaller area, may be utilized if voice is a necessity.

Security will become more of a concern as a larger portion of companies' critical information is made available to WLAN users. Network Managers will need to insure that the most up to date security measures are installed and monitored so that they are being used consistently within the network.

The ability to share access points across LAN subnetworks currently is being worked on, and standard solutions should be available soon. (Some installations currently use an ATM backbone network to create and support the subnetworks. The ATM system allows for access to multiple subnetworks.) Some terminals can be configured to log onto more than one network should this become necessary.

Companies developing WLAN products will need to be able to validate their products' performance in a variety of configurations. Some of the WLAN management products

discussed above have already demonstrated that they are useful tools in debugging and validating product performance.

However, as we have seen, effective management of WLANs is a critical concern. As installations get bigger, the size of the problem will get larger. RF performance, traffic loads and application of security measures will have to be routinely monitored and managed. As manufacturers bring out new products with additional RF and security options, assuring that all terminals are equipped with the right software releases and properly configured will be an ongoing problem. Recent product releases have automated some of this, but most solutions are still vendor proprietary. Monitoring the status of older products in a mobile terminal environment will be a major management activity in order to avoid user complaints to the system manager.

Network managers currently have the option to obtain centralized and/or portable network management tools. Centralized tools, integrated with the wired LAN management tools, will provide convenience and cost savings. They can see everything visible to the Access Point. However, if the Access Points do a lot of specialized monitoring to support performance analysis, they will reduce their capacity to handle customer traffic. These systems will probably stay limited to monitoring live traffic on their own network and managing equipment parameters. The addition of expert capabilities, which some vendors are already introducing, will make it easier to identify trouble spots and deduce the required remedial actions.

Portable devices will continue to be a necessary part of the network manager's toolkit. They will be necessary where peer-to-peer networks are permitted or to save costs in small, wireless only networks. But they also have a role in larger networks with centralized network management. Portable devices will play a major role in the deployment of additional network coverage. They will also be used to identify extraneous RF transmissions that may be creating areas of poor radio coverage. Moreover, they allow the manager to demonstrate that the RF coverage anticipated by the network architecture is actually being achieved. Portable devices also support auditing to verify that all of the security safeguards have been implemented at all of the critical network locations. They will catch rogue departments that have installed unauthorized local WLANS and attached them to the network.

Product evolution will continue to be a problem. Each new feature added could bring additional parameters that require management and monitoring. Centralized management tool manufacturers are supporting only their own equipment. The independent providers of portable test equipment would appear to have greater motivation, and an easier path, to providing tools that work across a mix of products. Users who expect to operate a mixture of WLAN products should carefully investigate the portable option and discuss their needs with the network management equipment vendor.

The new security standards being developed will require most existing equipment to be updated. Unfortunately, introduction of these important features means at least one more generation of equipment before these capabilities are available in the Access Point, the terminals and the management tools. It can be expected that manufacturers will continue to provide enhancements for their own WLAN products in order to gain a competitive advantage. While standards for network management are not yet a hot topic, one can

expect the Wireless LAN Association (WLANA) and the IEEE to ultimately react to this problem. It is only a matter of time before a standard set of MIBs and RF reporting capabilities are defined.

We can expect both centralized and portable network management systems to continue to add analysis capabilities as experience grows with the operation of 802.11b networks. Users will want their applications to work as well as they do on the desktop and will not want finger pointing between the wired and wireless segments. Managers will need tools to rapidly identify problems and test proposed solutions. The capabilities that are being added to network management tools today will make this easier to do tomorrow. In the mean time the promise of better things to come should not delay the adoption of WLAN technology today.

V. Appendix – Standards Activity

New 802 Family Standards- Security

The IEEE 802 family of standards includes both wired and wireless LANs. These standards have recognized the need to consider security. Wireless LANs are especially vulnerable to security attacks. It is possible to eavesdrop on, or spoof, a radio signal without a physical connection. In addition, portable laptops can readily be misplaced or stolen.

As the Internet experience is showing, hackers and industrial spies are constantly using new technologies to intercept or interfere with communications. New security patches and virus defenses are issued almost daily. The IEEE has been responding to this heightened level of concern by working on two new standards, 802.1x for all 802 LANs and 802.11e for WLANs.

802.1x

The IEEE 802.1x protocol is in the final approval process. This protocol defines changes to the operation of the MAC bridge to provide port based network access control. This will make it more difficult for unauthorized people to access the network. It will ultimately be issued as a supplement to IEEE standard 802.1D – 1998 (ISO/IEC 15802-3:1998). It will apply to 802.11, as well as other 802 LANs.

Among the advantages the IEEE 802.1x draft cites are: improved security, reduced complexity, enhanced scalability, superior availability, multicast propagation and end station manageability.

802.11e

The 802.11 standards group has been working on new QoS and security features. A recent study by a team of researchers at UC Berkeley has identified methods that could succeed in compromising the WLAN WEP protocol. The 802.11 security people have been aware of these vulnerabilities. Solutions were being codified in a new standard, 802.11e, that now may be released by early 2002 on an expedited schedule. The initial release will probably be known as WEP2. Since there is general agreement within the technical community as to what is needed, the WEP2 standard should be implemented rapidly. Users with a greater need can implement security at higher protocol layers to supplement the protection offered by WEP.

WEP2 will be applicable to all versions of 802.11. However, some of the new features are not compatible with the original WEP and implementation of the new features will require replacement or modification of existing network interface cards and access points.

802.11c

The IEEE 802.11c standard is a supplement to IEEE 802.1d that modifies this basic LAN standard to accommodate 802.11 frames. In particular it adds a sub clause under 2.5, *Support of the Internal Sublayer Service*, to cover bridge operations with 802.11 MACs.

Other Wireless Networking Standards

Three significant, and largely incompatible, wireless-networking standards are competing to use the 2.4 GHz ISM band in the United States. In addition to 802.11b, there are the Bluetooth and HomeRF systems. This complicates network design and management since the systems can interfere with each other when they are in the same physical area.

Bluetooth

Bluetooth, originally proposed as a replacement for short-range cabling, is a standard for wirelessly connecting a variety of terminal devices. It is intended to allow two terminals to interconnect at a very low price with high throughput. Since it uses RF spectrum, it does not have the same line of sight constraints as infrared. Many Bluetooth products have been announced in the last three months. Bluetooth capabilities are equivalent to some of those available with WLAN products.

Bluetooth uses frequency hopping spread spectrum. It is designed for low power consumption (which means a short range – nominally 30 feet), low cost and narrow bandwidth. (The gross data rate is 1 Mb/s.) The Bluetooth protocol specifically allows for voice channels. A Bluetooth system can support up to three voice channels, or a symmetric 432.6 kb/s data channel. Combinations of voice and data also can be supported. Authentication and 40- or 64-bit secret-key encryption may be activated if desired by the user.

Up to eight devices may be connected within a local network and up to eight networks may coexist in the same area. Multiple networks may coexist in the same space by using different frequency hopping sequences.

Several groups exist to support and further the Bluetooth standard. More information is available at www.bluetooth.com.

HomeRF

The HomeRF Shared Wireless Access Protocol (HomeRF SWAP) was intended to be a less costly version of the original IEEE 802.11 standard. It is a simplified implementation of IEEE 802.11's FHSS option, and was designed to reach price points acceptable to the home market. The HomeRF system includes features of the Digital Enhanced Cordless Telecommunications (DECT) standard in order to support both voice and data. The FCC has recently authorized HomeRF products to increase their transmission capabilities in order to support data rates up to 10 Mb/s. HomeRF incorporates a minimal level of authentication and supports encryption similar to GSM A5.

The Home Radio Frequency Working Group supports HomeRF SWAP. More information can be found at www.homerf.org.