Nokia Wireless LAN Products

WIRELESS LAN WHITE PAPER

TABLE OF CONTENTS

1. NOKIA WIRELESS LAN

Even though wireless LAN is new technology for Nokia, it is not dissimilar to the business where Nokia has been the leader since the technology was invented: data over the GSM network. As Nokia also has a wide background in all wireless telephony technologies and strong know-how in voice and data networks, entering the wireless LAN industry seems to be a logical step for a wireless connections specialist like Nokia.

2. WIRELESS LAN

A wireless LAN (WLAN) is a flexible data communication system implemented as an extension to a wired LAN within a building or campus. Using the radio frequency (RF) technology, WLANs transmit and receive data over the air, minimising the need for wired connections. WLAN provides users with mobile access to wired LANs in its coverage area.

Over the last seven years, WLAN has gained popularity in a number of vertical markets, including healthcare, retail, manufacturing, warehousing, and universities. These industries have profited from the productivity of using handheld terminals and laptop computers to transmit real-time information to centralised hosts for processing. The demand to use LAN facilities where ever you are, and working without complicated installations and cables, is increasing also in the everyday office environment. Standardisation of the wireless LAN technologies makes it more attractive to replace a part of traditional LANs with a wireless solution.

2.1 Wireless LAN applications

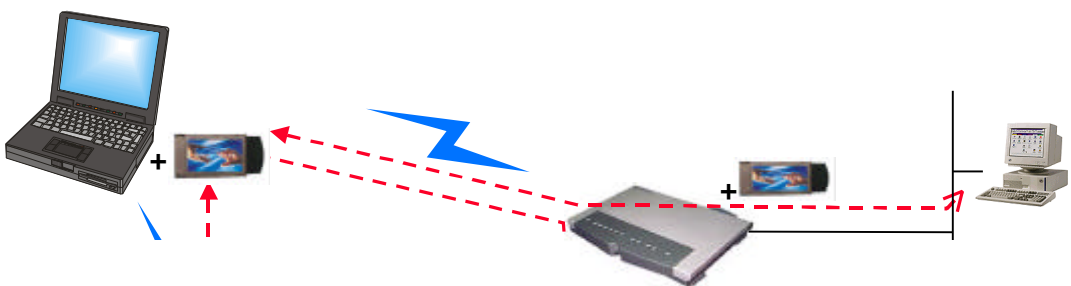
Wireless LAN applications have mainly been used in environments where using conventional PCs and wired LANs has been impractical or almost impossible. These environments include for example warehousing, retail stores, car rental agencies, and other special vertical solutions. The wireless LAN has provided a solution for many administrational problems in hospitals and a flexible connection method to schools and colleges.

These days the need for mobility is emerging also in other environments. Here are some examples of wireless LAN usage in everyday work.

2.1.1 Wireless meeting rooms

A continuously changing business environment requires greater flexibility from people and their working equipment. While some people always sit in front of their office PC, others may take part in several meetings during the working day. Too often these meetings are interrupted when participants leave the meeting room to obtain information, print slides or check to see if an important mail or fax message has arrived. This does not need to be the case anymore.

By expanding an existing LAN network with wireless LAN solutions to meeting rooms and shared areas, laptop computers can be used in the same way as the office desktops. With the peer-to-peer solution, people can share information with each other instantly.



Picture 1. The Instawave™ solution of Nokia

2.1.2 Wireless education

At schools and universities there is an increasing need to have access to shared databases and the Internet in classrooms and other shared areas. However, planning traditional networks for existing buildings and obtaining simple security solutions may be problematic.

With a wireless LAN on the campus and with laptop computers, classrooms and other areas can have flexible access to the network. Fixed desktop PCs are no longer needed. Laptop computers can be transferred from room to room as needed, and they can be collected in a single, secure location when not in use. Students can even bring their own laptops to the campus and have access to the needed databases and printers throughout the day.

A wireless LAN is easy to install and expand.

2.1.3 Wireless sales people

In small sales companies, most employees are at the office only once or twice a week as offices are often virtual. There is not enough physical office space for everybody, and employees spend much of their time in meetings. All IT support may be outsourced and remote connections are heavily used.

For this type of sites, wireless LAN solutions are easily provided through external IT support. All services can exist through Internet Providers or IT provider networks, and the office is only one connection to the IP/IT network. New laptop computers do not need to be installed on site, and the network can be easily expanded. The same security solutions that are used for remote connections can be used with a wireless LAN.

2.1.4 Wireless business centres

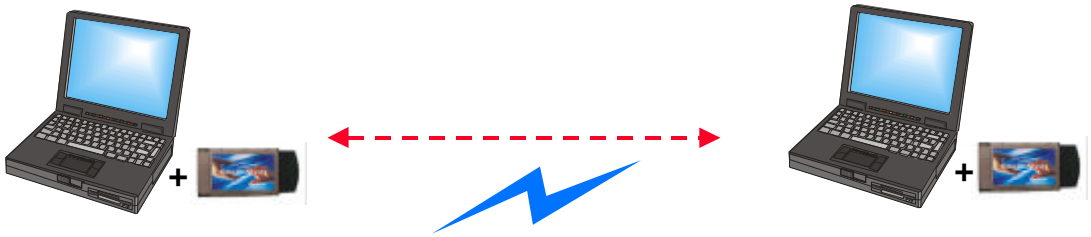
Conferences and large meetings that are arranged in hotels and business centres have always different requirements for the network, printers and projectors.

When this type of a site is equipped with a wireless LAN, participants can be given laptops to work with during the conference. They can also use their own computers via the wireless LAN. This way, they can print documents or use office services no matter in which meeting room or area they are located.

2.1.5 Wireless small offices

Many small offices require shared network services and information in network, but have no need or capacity for a complicated LAN infrastructure. The main requirements in this kind of environment are shared printing and Internet access.

Small offices benefit from a wireless LAN access point, which is able to handle outgoing data calls and use the Dynamic Host Configuration Protocol (DHCP). Also peer-to-peer networking is useful in small offices.



Picture 2. Peer-to-peer connection

3. WIRELESS LAN TECHNOLOGIES

Manufacturers of wireless LANs have a range of technologies to choose from when designing a wireless LAN solution. Each technology has its own advantages and limitations. Here is a short introduction to several wireless LAN technologies.

3.1 Narrowband technology

A narrowband radio system transmits and receives user information on a specific radio frequency. The narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. Undesirable crosstalk between communications channels is avoided by carefully co-ordinating users on different channel frequencies.

A private telephone line is much like a radio frequency. When each house has its own private telephone line, people in one house cannot listen to calls made to the other house. In a radio system, privacy and non-interference are accomplished by using separate radio frequencies. The radio receiver filters out all radio signals except the ones on its designated frequency.

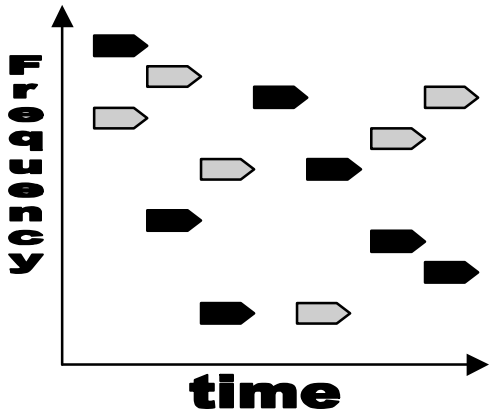
3.2 Spread spectrum

Most wireless LAN systems use the spread spectrum technology, a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. Spread spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security. In other words, more bandwidth is consumed than in narrowband transmission, but the

trade-off produces a signal that is louder and thus easier to detect, provided that the receiver knows the parameters of the spread spectrum signal being broadcast. If the receiver is not tuned to the right frequency, a spread spectrum signal looks like background noise. There are two types of spread spectrum radio: frequency hopping and direct sequence.

3.3 Frequency hopping spread spectrum technology

Frequency hopping spread spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both the transmitter and the receiver. Properly synchronised, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

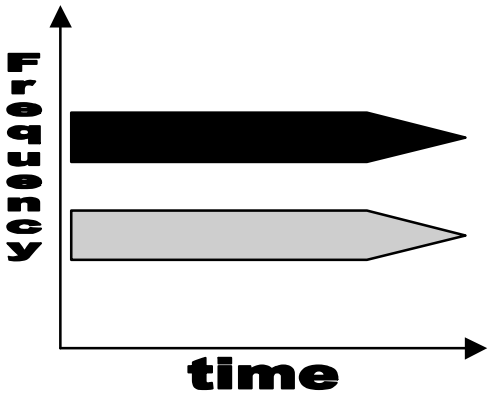


Picture 3. FHSS

3.4 Direct sequence spread spectrum technology

Direct sequence spread spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered (and, of course, the more bandwidth required). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is rejected or ignored by most narrowband receivers.

With DSSS, the normal data rates in IEEE802.11 are 1, 2, 5.5 and 11 Mbps. The 11 Mbps rate also enables the use of multimedia solutions.



Picture 4. DSSS

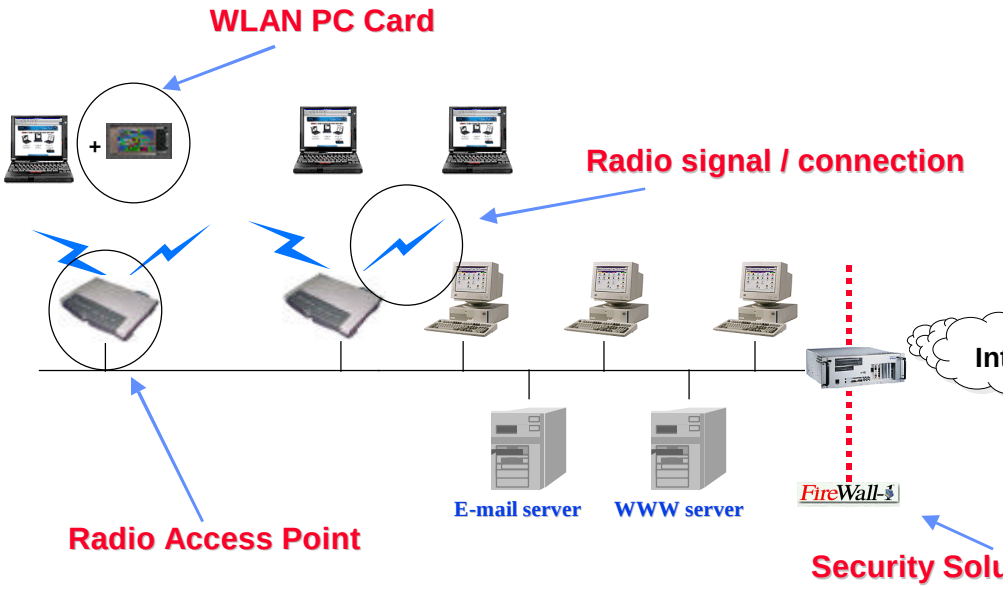
4. HOW WIRELESS LANS WORK

Wireless LANs use electromagnetic airwaves (radio and infrared) to transfer information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers, because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier.

Multiple radio carriers can exist in the same space at the same time without interfering each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver or augment networks without installing or moving wires. Wireless LANs tunes to (or selects) one radio frequency while rejecting all other radio signals on different frequencies.

In a typical WLAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location using a standard Ethernet cable. At a minimum, the access point receives, buffers, and transmits data between the WLAN and the wired network. A single access point can support a small group of users and can function within a range from less than one hundred to several hundred feet. The access point (or the antenna attached to the access point) is usually mounted high, but it may be mounted on any practical place as long as the desired radio coverage is obtained.

End users access the WLAN through wireless LAN adapters, which are implemented as PC cards in laptop computers, ISA or PCI cards in desktop computers, or integrated within handheld computers. WLAN adapters provide an interface between the client network operating system (NOS) and the airwaves (via an antenna). The nature of the wireless connection is transparent to the NOS.



Picture 3 Wireless LAN network

4.1 WLANs & other wireless technologies

Wireless LANs provide all the functionality of wired LANs, but without the physical constraints of the wire itself. Wireless LAN configurations include independent networks offering peer-to-peer connections, and infrastructure networks supporting fully distributed data communications. Point-to-point local area wireless solutions, such as LAN-to-LAN bridging and personal area networks (PANs), may overlap with some WLAN applications, but they fundamentally address different user needs. A wireless LAN-to-LAN bridge is an alternative to a cable that connects LANs in two separate buildings. A wireless PAN typically covers the few feet surrounding a user's work space and enables synchronising computers, transferring files, and accessing local peripherals.

Wireless LANs should not be confused with wireless metropolitan area networks (WMANs), which are packet radio systems often used for law enforcement or utility applications, or with wireless wide area networks (WWANs), which transmit wide area data transmission over cellular or packet radio. These systems involve expensive infrastructures, provide much lower data rates, and require users to pay for the bandwidth on a time or usage basis. In contrast, on-premise wireless LANs require no usage fees and provide 100-1000 times the data transmission rate.

5. BENEFITS OF WLANS

Wireless LANs provide flexible installation and configuration and mobility in network environment. Key issues in implementing a wireless LAN are coverage, throughput, interoperability with wired infrastructure, network management, security, cost, and ease of use.

5.1.1 Range and coverage

The distance over which RF and IR waves can communicate depends on product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, such as walls, metal, and even people, can affect the propagation of energy, and thus also the range and coverage of the system. IR is blocked by solid objects, which provides additional limitations. Most wireless LAN systems use RF, because radio waves can penetrate many indoor walls and surfaces. The range for typical WLAN systems varies from under 100 feet to more than 300 feet. Coverage can be extended, and true freedom of mobility achieved via roaming, provided through microcells. For more information, see the Wireless Network white paper of Nokia.

5.1.2 Throughput

As with wired LAN systems, the actual throughput in wireless LANs depends on the product and set-up. Factors that affect the throughput include the number of users, propagation factors, such as range and multipath, the type of WLAN system used, as well as the latency and bottlenecks on the wired parts of the WLAN. Typical data rates range from 1 to 11 Mbps. Users of traditional wired LANs generally experience little difference in performance when using a wireless LAN and can expect similar latency behaviour. Wireless LANs provide sufficient throughput for the most common LAN-based office applications, including electronic mail exchange, access to shared peripherals, and access to multi-user databases and applications.

5.1.3 Interoperability with wired infrastructure

Wireless data technologies have been tested for more than 50 years in both commercial and military systems. While radio interference can cause degradation in throughput, such interference is rare in the workplace. Robust designs of tested WLAN technology and the limited distance over which signals travel, result in connections that are far more robust than cellular phone connections, and they provide data integrity performance equal to or better than wired networking.

5.1.4 Interoperability with wireless infrastructure

There are several types of possible interoperability between wireless LANs. They depend both on the chosen technology and on the implementation of a specific vendor. Products from different vendors using the same technology and the same implementation typically allow interchange between adapters and access points. The main goal of the IEEE802.11 specification, currently being drafted by a committee of WLAN vendors and users, is to allow compliant products to interoperate without explicit collaboration between vendors.

5.1.5 Interference and co-existence

The unlicensed nature of radio-based wireless LANs means that other products transmitting energy in the same frequency spectrum can potentially provide some interference to a WLAN system. Microwave ovens are a potential concern, but most WLAN manufacturers design their products to account for microwave interference. Another concern is the co-location of multiple WLANs. While WLANs from some manufacturers interfere with other WLANs, others co-exist without interference. This issue is best addressed directly with the appropriate vendors.

5.1.6 Simplicity and ease of use

Users need very little new information to take advantage of wireless LANs. Because the wireless nature of a WLAN is transparent to a user's NOS, applications work in the same way as they do on

tethered LANs. WLAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system. However, most products are designed so that users rarely need these tools.

WLANs simplify many of the installation and configuration issues that cause problems to network managers. Since only the access points of WLANs require cabling, network managers are freed from pulling cables for WLAN end users. The lack of cabling in the wireless LAN system makes moving, addtions, and changes trivial operations. Finally, the portability of WLANs lets network managers pre-configure and troubleshoot entire networks before installing them at remote locations. Once configured, WLANs can be moved from place to place with little or no modification.

5.1.7 Security

Because the wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into wireless LANs, making them more secure than most wired LANs. Complex encryption techniques make it impossible for all but the most sophisticated systems to gain unauthorised access to network traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic. For more information, see the General Wireless LAN security white paper of Nokia.

5.1.8 Network management

When implementing a wireless LAN to a wired LAN infrastructure, existing network management solutions should be taken into account. Most wireless LAN access points support the standard network protocols TCP/IP, NetBEUI, and IPX. They can be managed with different network management tools, which support the Simple Network Management Protocol (SNMP). Setting up a suitable wireless LAN to a wired LAN should not require tool changes or additions in network management systems.

5.1.9 Cost

Setting up a wireless LAN includes both infrastructure costs for the wireless access points, and user costs for the wireless LAN adapters. The infrastructure costs depend primarily on the number of access points deployed. The number of access points typically depends on the required coverage area and/or the number and type of users to be served. The coverage area is proportional to the square of the product range. Wireless LAN adapters are required for standard computer platforms.

The cost of installing and maintaining a wireless LAN generally is lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, WLAN eliminates the direct costs of cabling and the labour associated with installing and repairing it. Second, because WLANs simplify moving, additions, and changes, the indirect costs of user downtime and administrative overhead are reduced.

5.1.10 Scalability

Wireless networks can be designed to be extremely simple or complex. Wireless networks can support large numbers of nodes and/or large physical areas by adding access points to boost or extend coverage. For more information, see the Wireless Network white paper of Nokia.

5.1.11 Battery life for mobile platforms

End-user wireless products are designed to run off the AC or battery power from their host laptop or handheld computer, since they have no direct wire connection of their own. WLAN vendors typically employ special design techniques to maximise the host computer's energy usage and battery life.

5.1.12 Safety

The output power of wireless LAN systems is very low, much less than that of a mobile phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a wireless LAN system. Wireless LANs must meet stringent government and industry regulations for safety. No adverse health effects have ever been attributed to wireless LANs.

6. SUMMARY

Wireless LAN offers the user more flexibility and security. It is seamless to use; no new software is needed. Wireless LAN enables mobility in campus areas with the same data rate and services of a wired LAN but without attached cables.

With a wireless LAN, IT personnel need not spend their time in maintaining cables or other fixed systems when the users change their locations. All devices can be installed in one single location, no matter where they will be used in the wireless LAN. A wireless LAN is easy to extend.

A wireless LAN is not much more expensive than a wired LAN, and the maintenance costs are even lower.

There is no other network solution that is as flexible, secure and easy to implement as the wireless LAN.

This document is based on Wireless LAN Alliance's publication "Introduction to Wireless LANs" with the permission of the Wireless LAN Alliance.

WLAN Glossary

Access point
: A device that transfers data between a wireless network and a wired network.

IEEE802.X
: A set of specifications for Local Area Networks from the Institute of Electrical and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks or 802.5 the specification for token ring networks. There is an 802.11 committee working on a standard for 1 and 2 Mbps wireless LANs. The standard will have a single MAC layer for the following physical-layer technologies: Frequency Hopping Spread Spectrum, Direct Sequence Spread Spectrum, and Infrared. Draft versions of the specification are in process.

Independent network
: A network that provides (usually temporarily) peer-to-peer connectivity without relying on a complete network infrastructure.

Infrastructure network
: A wireless network centered about an access point. In this environment, the access point not only provides communication with the wired network but also mediates wireless network traffic in the immediate neighborhood.

Microcell
: A bounded physical space in which a number of wireless devices can communicate. Because it is possible to have overlapping cells as well as isolated cells, the boundaries of the cell are established by some rule or convention.

Radio Frequency (RF) Terms: GHz, MHz, Hz
: The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One Mega-Hertz (MHz) is one million Hertz. One Giga-Hertz (GHz) is one billion Hertz. For reference: the standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55 -1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and microwave ovens typically operate at 2.45 GHz.

Roaming
: Movement of a wireless node between two microcells. Roaming usually occurs in infrastructure networks built around multiple access points.

Wireless node
: A user computer with a wireless network interface card.

GSM
: Global System for Mobile Communications

SNMP
: Simple Network Management Protocol