Chapter 8:
Wireless Networking Concepts

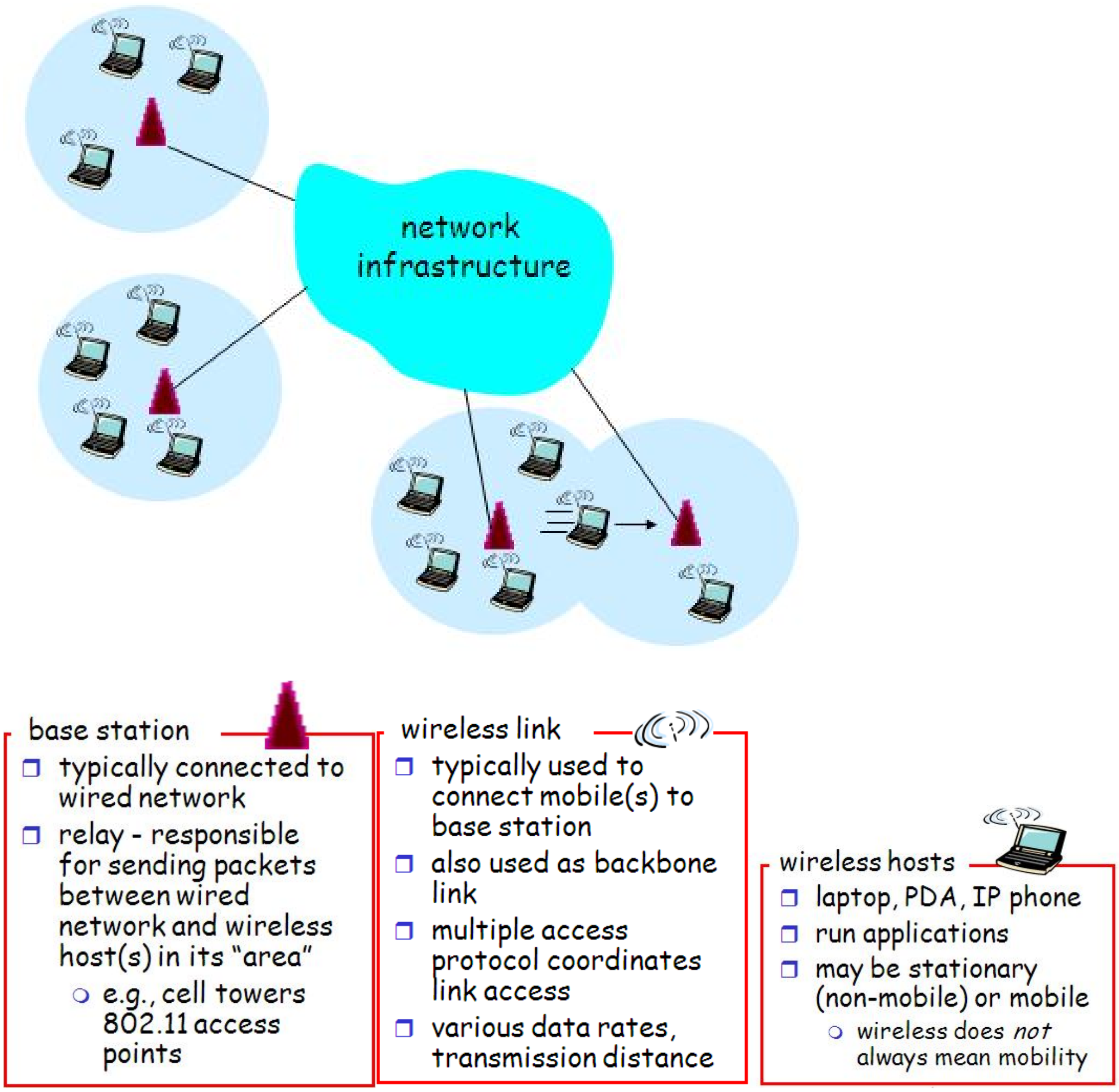
8.1 Wireless Networks

Wireless networks serve as the transport mechanism between devices and among devices and the traditional wired networks (enterprise networks and the Internet). Wireless networks are many and diverse but are frequently categorized into three groups based on their coverage range: **Wireless Wide Area Networks** (**WWAN**), **WLANs**, and **Wireless Personal Area Networks** (**WPAN**).

WWAN includes wide coverage area technologies such as 2G cellular, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), and Mobitex. WLAN, representing wireless local area networks, includes 802.11 (Wi-Fi), Hiper LAN, and several others. WPAN represents wireless personal area network technologies such as Bluetooth and IR.

All of these technologies are "tetherless"—they receive and transmit information using electromagnetic (EM) waves. Wireless technologies use wavelengths ranging from the radio frequency (RF) band up to and above the IR band. The frequencies in the RF band cover a significant portion of the EM radiation spectrum, extending from 9 kilohertz (kHz), the lowest allocated wireless communications frequency, to thousands of gigahertz (GHz). As the frequency is increased beyond the RF spectrum, EM energy moves into the IR and then the visible spectrum.

8.2 Elements of a Wireless Network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers 802.11 access points

wireless link

- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

wireless hosts

- laptop, PDA, IP phone
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility

Figure 8.1 Elements of a wireless network.

The basic elements of a wireless network are:

- **Access Point** (or **Base S**tation): a device that connects wireless communication devices together to form a wireless network. The WAP usually connects to a wired network, and can relay data between wireless devices and wired devices. Several WAPs can link together to form a larger network that allows "roaming". WAPs have IP addresses for configuration. There are two types of access points:

1- Dedicated **Hardware Access Points** (**HAP**) such as Lucent's WaveLAN, Apple's Airport Base Station, Linksys, 3com or WebGear's AviatorPRO. Hardware access points offer comprehensive support of most wireless features.

2- **Software Access Points** which run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network. The Vicomsoft InterGate suites are software routers that can be used as a basic Software Access Point, and include features not commonly found in hardware solutions, such as Direct PPPoE support and extensive configuration flexibility, but may not offer the full range of wireless features defined in the 802.11 standard.

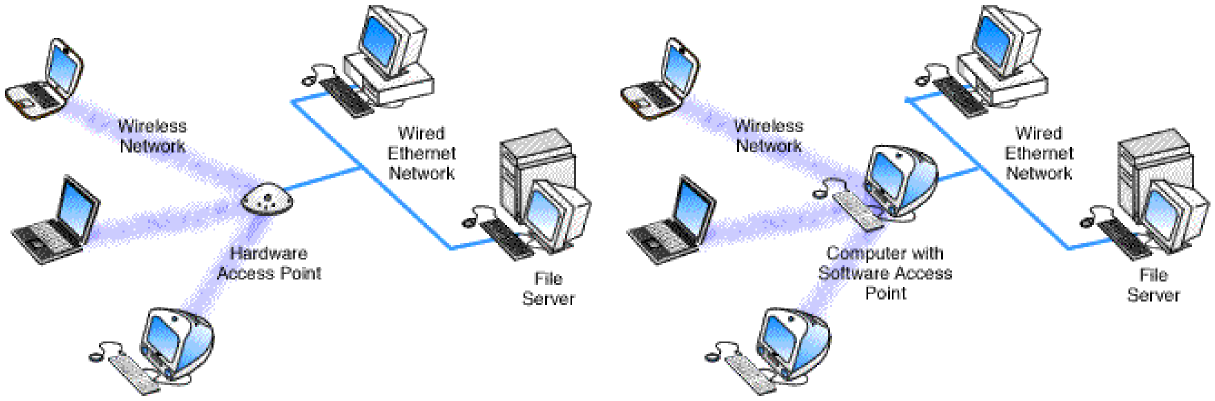


Figure 8.2 Comparing Software Access Point and Hardware Access Point.

- **Wireless Link**: is used to connect the different wireless devices together. It has various data rates and protocols. Also used within a network to connect routers, switches and other network equipment.
- **Wireless Hosts**: usually means the different devices (laptops and PDAs) interconnected in a network. The devices may be stationary or mobile and this shall be discussed later.

8.3 Ad Hoc and Infrastructure Networks

Wireless networks may be classified according to their structures into **Ad Hoc Networks** and **Infrastructure Networks**.

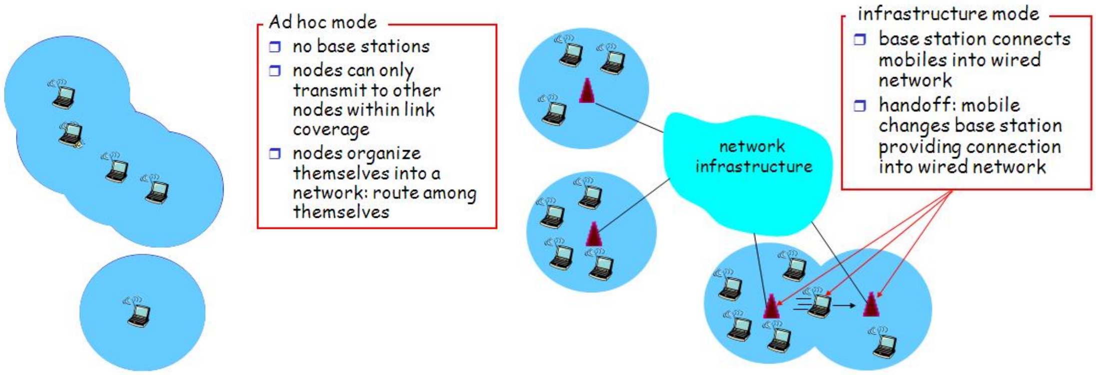

Ad hoc mode
❐ no base stations
❐ nodes can only transmit to other nodes within link coverage
❐ nodes organize themselves into a network: route among themselves
network infrastructure
infrastructure mode
❐ base station connects mobiles into wired network
❐ handoff: mobile changes base station providing connection into wired network

Figure 8.3 Comparing Ad hoc mode and infrastructure mode.

A wireless ad-hoc network, also known as **IBSS** - **Independent Basic Service Set**, is a computer network in which the communication links are wireless. The network is ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to older network technologies, which we shall see discuss in the next paragraph, in which some designated nodes, usually with custom hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc.

In infrastructure mode, a wireless network uses an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.

In our project we have chosen to control and monitor our processes via infrastructure mode since its installation needs less configuration (whereas ad-hoc mode requires setting the SSID for each device) as well as providing more flexibility since an AP may easily allow us to connect to a wired network as well as easily identifying any new wireless host.

8.4 Wireless Standards

Wireless technologies conform to a variety of standards and offer varying levels of security features. The principal advantages of standards are to encourage mass production and to allow products from multiple vendors to interoperate. Each protocol is defined in IEEE standards. WLANs or Wi-Fi follow the IEEE 802.11 standards, Bluetooth follows IEEE 802.15.1 while Zigbee follows IEEE 802.15.4. Ad hoc networks follow proprietary techniques or are based on the Bluetooth standard, which was developed by a consortium of commercial companies making up the Bluetooth Special Interest Group (SIG). These standards are described below.

The IEEE 802 standards typically create the specifications at the physical layer and portions of the data link layer. The higher layer protocols are left to the industry and the individual applications. Hence the standard and market names are not always interchangeable.

8.4.1 Wi-Fi

Wi-Fi or WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1998. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations.

802.11 is the original WLAN standard, designed for 1 Mbps to 2 Mbps wireless transmissions. It was followed in 1999 by 802.11a, which established a high-speed WLAN standard for the 5 GHz band and supported 54 Mbps. Also completed in 1999 was the 802.11b standard, which operates in the 2.4 - 2.48 GHz band and supports 11 Mbps. The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's applications. Because the 802.11b standard has been so widely adopted, the security weaknesses in the standard have been exposed. Another standard, 802.11g, still in draft, operates in the 2.4 GHz wave band, where current WLAN products based on the 802.11b standard operate.

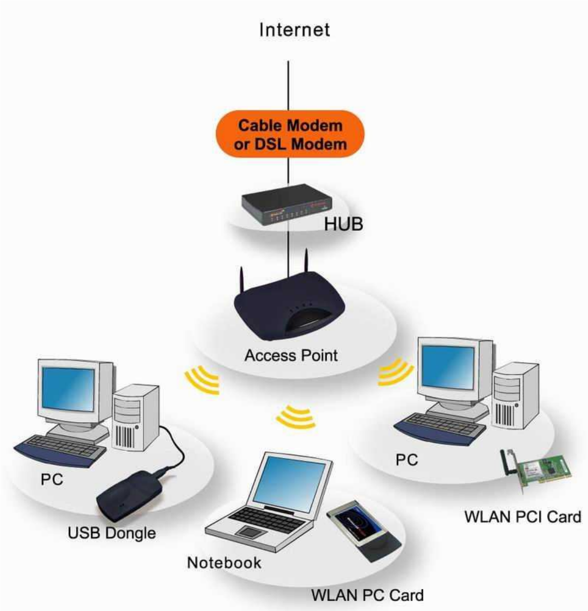


Figure 8.4 An example of a wireless LAN connected to the Internet.

Two other important and related standards for WLANs are 802.1X and 802.11i. The 802.1X, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks.

We have chosen this standard in our projects in order to be compatible with most devices found in the market as well as its ability to interface smoothly with wired Ethernet networks and the Internet.

Characteristic	Description
Physical Layer	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Orthogonal Frequency Division Multiplexing (OFDM), Infrared (IR).
Frequency Band	2.4 GHz (ISM band) and 5 GHz.
Data Rates	1 Mbps, 2 Mbps, 5.5 Mbps (11b), 11 Mbps (11b), 54 Mbps (11a)
Data and Network Security	RC4-based stream encryption algorithm for confidentiality, authentication and integrity. Limited key management. (AES is being considered for 802.11i.)
Operating Range	Up to 150 feet indoors and 1500 feet outdoors.
Positive Aspects	Ethernet speed without wires; many different products from many different companies. Wireless client cards and access point costs are decreasing.
Negative Aspects	Poor security in native mode; throughput decrease with distance and load.

Table 8.2 Key characteristics of 802.11 WLANs.

8.4.2 Bluetooth

Bluetooth has emerged as a very popular ad hoc network standard today. The Bluetooth standard is a computing and telecommunications industry specification that describes how mobile phones, computers, and PDAs should interconnect with each other, with home and business phones, and with computers using short-range wireless connections. The Bluetooth standard specifies wireless operation in the 2.45 GHz radio band and supports data rates up to 820 kbps. It further supports up to three simultaneous voice channels and employs frequency-hopping schemes and power reduction to reduce interference with other devices operating in the same frequency band. The IEEE 802.15 organization has derived a wireless personal area networking technology based on Bluetooth specifications v1.1.

Ad hoc networks today are based primarily on Bluetooth technology. Bluetooth is an open standard for short-range digital radio. It is touted as a low-cost, low-power, and low-profile technology that provides a mechanism for creating small wireless networks on an ad hoc basis. Bluetooth is considered a wireless PAN technology that offers fast and reliable transmission for both voice and data. Untethered Bluetooth devices will eliminate the need for cables and provide a bridge to existing networks.

Bluetooth can be used to connect almost any device to any other device. An example is the connection between a PDA and a mobile phone. The goal of Bluetooth is to connect disparate devices (PDAs , cell phones , printers, faxes, etc.) together wirelessly in a small environment such as an office or home. According to the leading proponents of the technology, Bluetooth is a standard that will ultimately—

- Eliminate wires and cables between both stationary and mobile devices
- Facilitate both data and voice communications
- Offer the possibility of ad hoc networks and deliver synchronicity between personal devices.

Bluetooth is designed to operate in the unlicensed ISM (industrial, scientific, medical applications) band that is available in most parts of the world, with variation in some locations. The characteristics of Bluetooth are summarized in Table 8.3. Bluetooth-enabled devices will automatically locate each other, but making connections with other devices and forming networks requires user action. As with all ad-hoc networks, Bluetooth network topologies are established on a temporary and random basis.

A distinguishing feature of Bluetooth networks is the master-slave relationship maintained between the network devices. Up to eight Bluetooth devices may be networked together in a master-slave relationship, called a **piconet**. In a piconet, one device is designated as the master of the network with up to seven slaves connected directly to that network. The master device controls and sets up the network (including defining the network's hopping scheme). Devices in a Bluetooth piconet operate on the same channel and follow the same frequency hopping sequence. Although only one device may perform as the master for each network, a slave in one network can act as the master for other networks, thus creating a chain of networks. This series of piconets, often referred to as **scatter-nets**, allows several devices to be inter-networked over an extended distance. This relationship also allows for a dynamic topology that may change during any given session: as a device moves toward or away from the master device in the network, the topology and therefore the relationships of the devices in the immediate network change.

Characteristic	Description
Physical Layer	Frequency Hopping Spread Spectrum (FHSS)
Frequency Band	2.4 – 2.4835 GHz (ISM band).
Hop Frequency	1600 hops/sec.
Data Rates	1 Mbps (raw). Higher bit rates are anticipated.
Data and Network Security	Three modes of security (none, link-level and service-level), two levels of device trust, and three levels of service security. Stream encryption for confidentiality, challenge response for authentication. PIN-derived keys and limited management.
Operating Range	About 10 meters (30 feet); can be extended to 100 meters.
Throughput	Up to approximately 820 kbps.
Positive Aspects	No wires and cables for many interfaces. Ability to penetrate walls and other obstacles. Costs are decreasing with a $5 cost projected. Low power and minimal hardware.
Negative Aspects	Possibility for interference with other ISM band technologies. Relatively low data rates. Signal leak outside desired boundaries.

Table 8.3 Key characteristics of Bluetooth.

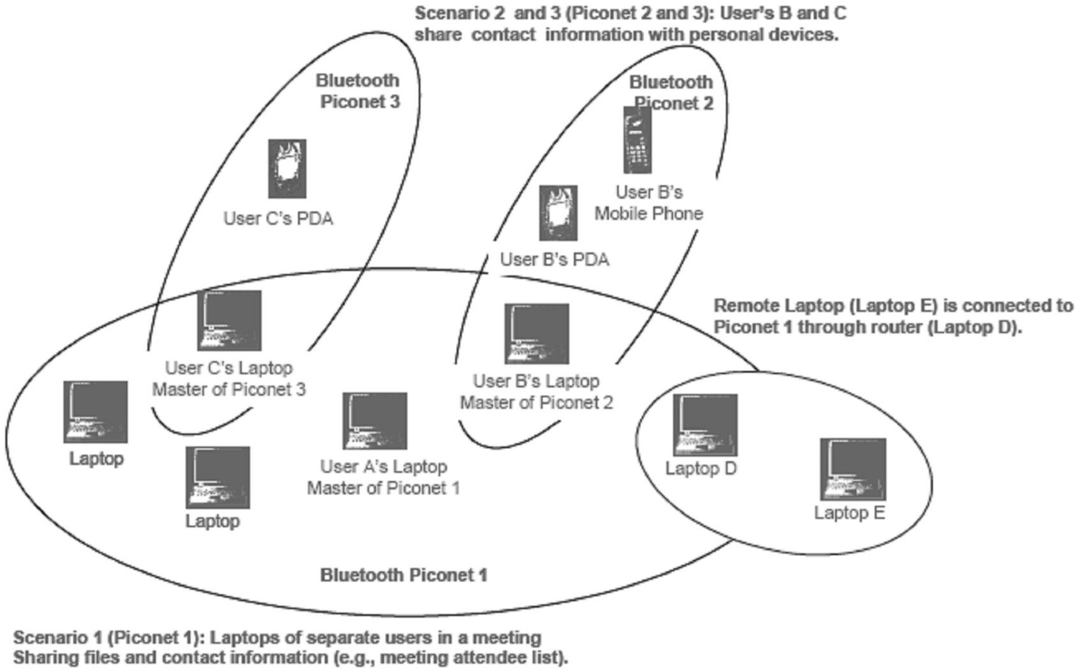

Scenario 2 and 3 (Piconet 2 and 3): User's B and C share contact information with personal devices.
Bluetooth Piconet 3
Bluetooth Piconet 2
User C's PDA
User B's Mobile Phone
User B's PDA
Remote Laptop (Laptop E) is connected to Piconet 1 through router (Laptop D).
User C's Laptop Master of Piconet 3
User B's Laptop Master of Piconet 2
Laptop
Laptop
User A's Laptop Master of Piconet 1
Laptop D
Laptop E
Bluetooth Piconet 1
Scenario 1 (Piconet 1): Laptops of separate users in a meeting Sharing files and contact information (e.g., meeting attendee list).

Figure 8.5 Typical Bluetooth Network—A Scatter-net.

Mobile routers in a Bluetooth network control the changing network topologies of these networks. The routers also control the flow of data between devices that are capable of supporting a direct link to each other. As devices move about in a random fashion, these networks must be reconfigured on the fly to handle the dynamic topology. The routing protocols it employs allow Bluetooth to establish and maintain these shifting networks.

Bluetooth transceivers operate in the 2.4 GHz, ISM band, which is similar to the band WLAN devices and other IEEE 802.11 compliant devices occupy. Bluetooth transceivers, which use Gaussian Frequency Shift Keying (GFSK) modulation, employ a frequency hopping (FH) spread spectrum system with a hopping pattern of 1,600 times per second over 89 frequencies in a quasi-random fashion. The theoretical maximum bandwidth of a Bluetooth network is 1 Mbps. However, in reality the networks cannot support such data rates because of communication overhead. The second generation of Bluetooth technology is expected to provide a maximum bandwidth of 2 Mbps.

Bluetooth networks can support either one asynchronous data channel with up to three simultaneous synchronous speech channels or one channel that transfers asynchronous data and synchronous speech simultaneously. Bluetooth uses a combination of packet-switching technology and circuit-switching technology. The advantage of using packet switching in Bluetooth is that it allows devices to route multiple packets of information by the same data path. Since this method does not consume all the resources on a data path, it becomes easier for remote devices to maintain data flow throughout a scatter-net.

Clearly, Bluetooth is not suitable for industrial due to its short-distance range and support for limited number of nodes.

8.4.3 ZigBee

ZigBee is built on top of the IEEE 802.15.4 standard. ZigBee provides routing and multi-hop functions to communication. **ZigBee** is the name of a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks (WPANs). ZigBee is targeted at RF applications that require a low data rate, long battery life, and secure networking.

ZigBee Key Features:

- **Low Power**

  Low power is one of the key aspects of ZigBee. 802.15.4 was chosen due to it's low power requirements. 802.15.4 radios have the capability to come from an off state to be on the network and transmitting in less then 30ms. This allows the radio to be turned off and powered on only when needed, providing the lowest possible system power. Compare this too many radios that need to remain synchronized with the network or take up to several seconds to connect and transmit from an off state. This delay would be unacceptable for applications such as lighting were requirements are less then 100ms. In addition, during the time the radios are staring up, they are consuming extra power. When combined with Freescale's low power MCUs, 802.15.4 and ZigBee have the potential to last as long as the shelf life of most batteries.

- **Robust**

802.15.4 provides a robust foundation for ZigBee, ensuring a reliable solution in noisy environments. Features such as energy detection, clear channel assessment and channel selection help the device pick the best possible channel, avoiding other wireless networks such as Wi-Fi®. Message acknowledgement helps to ensure that the data was delivered to its destination. Finally, multiple levels of security ensure that the network and data remain intact and secure.

- **Mesh Networking**

The ability to cover large areas with routers is one of the key features of ZigBee that helps differentiate itself from other technologies. Mesh networking can extend the range of the network through routing, while self healing increases the reliability of the network by re-routing a message in case of a node failure

- **Interoperability**

The ZigBee Alliance helps ensure interoperability between vendors by creating testing and certification programs for ZigBee devices. Users can be assured the devices that go through certification testing and use the ZigBee logo will work with other devices based on the same applications. This provides end customers with the customers with peace of mind while creating brand awareness of products with the ZigBee logo.

Freescale offers a comprehensive ZigBee solution, including RF chipsets, MCUs, sensors, reference designs, protocol stack software, and development tools. For more information on our ZigBee Family offering see www.freescale.com/zigbee.

However, since we wanted to provide both Ethernet and wireless accessibility, we chose to use Wi-Fi rather than ZigBee since the difference in bit rates between Ethernet and ZigBee is greater than that between Ethernet and Wi-Fi. Using ZigBee might have caused problems in transmissions causing less throughput and probably buffer problems.

The relationship between IEEE 802.15.4-2003 and ZigBee is similar to that between IEEE 802.11 and the Wi-Fi Alliance. The ZigBee 1.0 specification was ratified on December 14, 2004 and is available to members of the ZigBee Alliance. An entry level membership, called Adopter, in the ZigBee Alliance costs US$ 3500 annually and provides access to the specifications and permission to create products for market using the specifications. For non-commercial purposes, the ZigBee specification is available to the general public at the ZigBee Specification Download Request. Most recently, the ZigBee 2006 specification was posted in December 2006.

ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and 2.4 GHz in most jurisdictions worldwide. The technology is intended to be simpler and cheaper than other WPANs such as Bluetooth. The most capable ZigBee node type is said to require only about 10% of the software of a typical Bluetooth or Wireless Internet node, while the simplest nodes are about 2%. However, actual code sizes are much higher, closer to 50% of Bluetooth code size. ZigBee chip vendors have announced 128 kilobyte devices

ZigBee protocols are intended for use in embedded applications requiring low data rates and low power consumption. ZigBee's current focus is to define a general-purpose, inexpensive, self-organizing, mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, domotics, etc. The resulting network will use very small amounts of power so individual devices might run for a year or two using the originally installed battery.

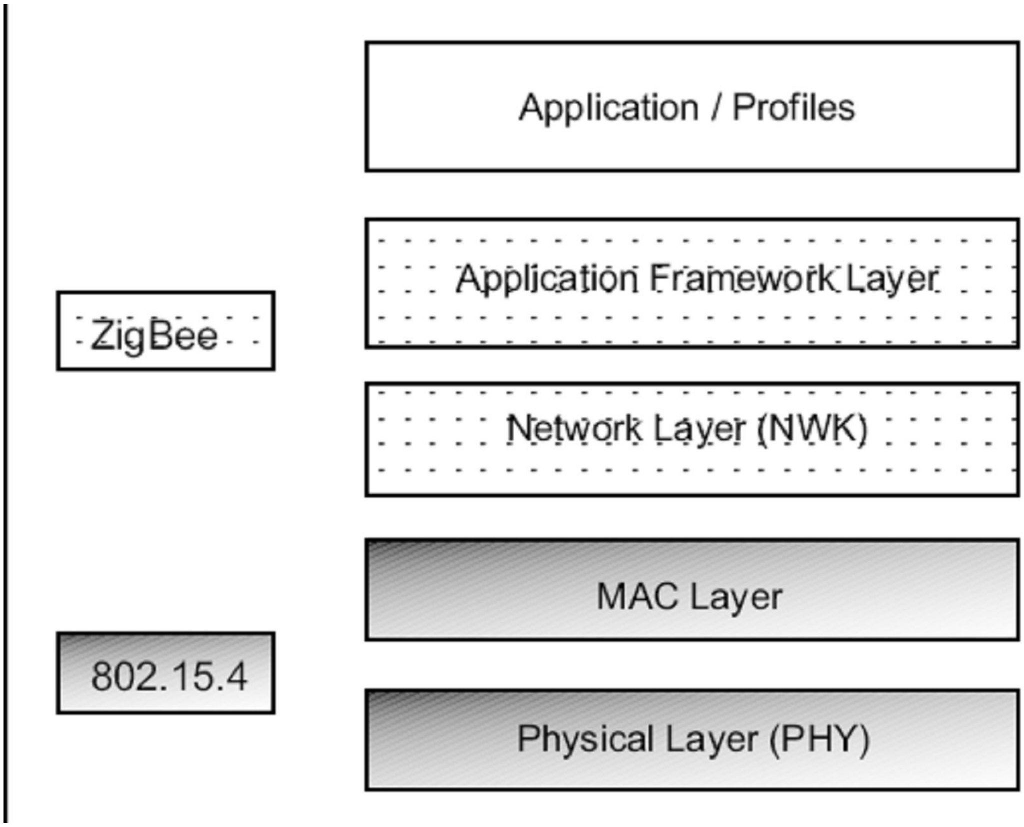


Figure 8.6 ZigBee Stack

8.5 UDP or TCP Over Wireless

During our work, we have discovered that the performance of the UDP protocol over wireless LAN is much lower than that of TCP. Therefore, despite UDP's advantages of having lower overhead, faster response and the need for less complex code (due to its connectionless nature and the absence of handshaking), we had to use TCP protocol in our project.

Tests done by Center for Wireless Communications & Computer Systems Laboratory, Department of Computer Science & Engineering at the University of California, San Diego have agreed with our observation. In their tests, they added an option for UDP tests that uses packet sequence numbers so that the receiver can detect and report packet losses (as they occur and in total), and named this version ettcp.

Their results noticed that in *all* UDP tests with 100 byte packets, 90-95% of packets sent by `ettcp` were never transmitted, and actually did not even reach the interface according to the driver. The reason was buffer shortages at the UDP level, due to the very fast generation rate of short packets, which caused datagrams to be dropped. When running the same tests over the faster wired interfaces for comparison purposes, fewer packets (50%) were dropped as expected. TCP tests with 100 byte packets did not suffer from such drops, because TCP uses window based flow control, with a maximum window of 32 KB in the tests. This prohibits the sending process from passing to the network code huge bursts of data without pause. Even though `ettcp` used a TCP socket option to transmit data segments immediately, they occasionally saw packets larger than expected, except in the 1500 byte packet tests where the maximum WLAN packet size was reached. The reason is that TCP keeps track of its transmission queue in terms of bytes rather than packets, thus any segments whose immediate transmission is deferred may be later combined into larger packets. Such delays can be caused by MAC layer contention due to the bidirectional traffic of TCP.

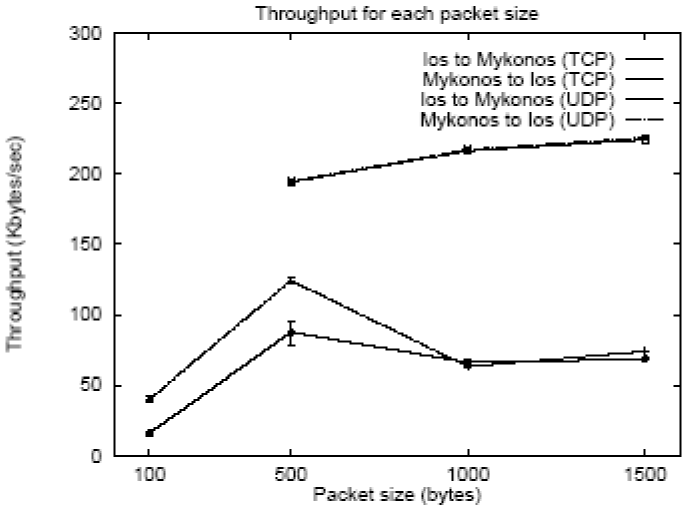


Figure 8.7 Part of the results of the tests done by Center for Wireless Communications & Computer Systems Laboratory at the University of California, showing that the throughput of TCP was higher than that of UDP.

8.6 Roaming

A wireless computer can "roam" from one access point to another, with the software and hardware maintaining a steady network connection by monitoring the signal strength from in-range access points and locking on to the one with the best quality. Usually this is completely transparent to the user; they are not aware that a different access point is being used from area to area. Some access point configurations require security authentication when swapping access points, usually in the form of a password dialog box. Access points are required to have overlapping wireless areas to achieve this as can be seen in the following diagram:

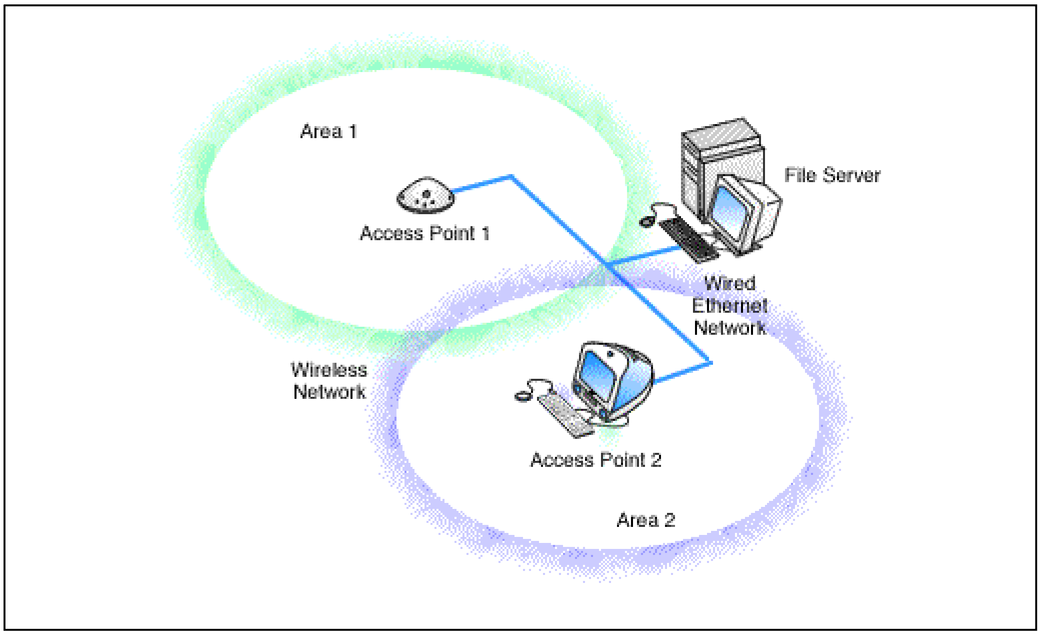


Figure 8.8 Roaming

A user can move from Area 1 to Area 2 transparently. The Wireless networking hardware automatically swaps to the Access Point with the best signal. This handshaking is done by the operating system of the wireless host.

8.7 Ethernet to Wireless Conversion

The microcontroller which we have used, HCS12NE64, provides us with Ethernet connectivity not wireless connectivity. In order to achieve wireless connectivity, we had to find a bridge to convert the Ethernet protocol to the wireless Wi-Fi protocol. This conversion only affects the physical and data-link layer, therefore, the other functions in the upper layers will not be changed and therefore we have achieved transparency between the devices.

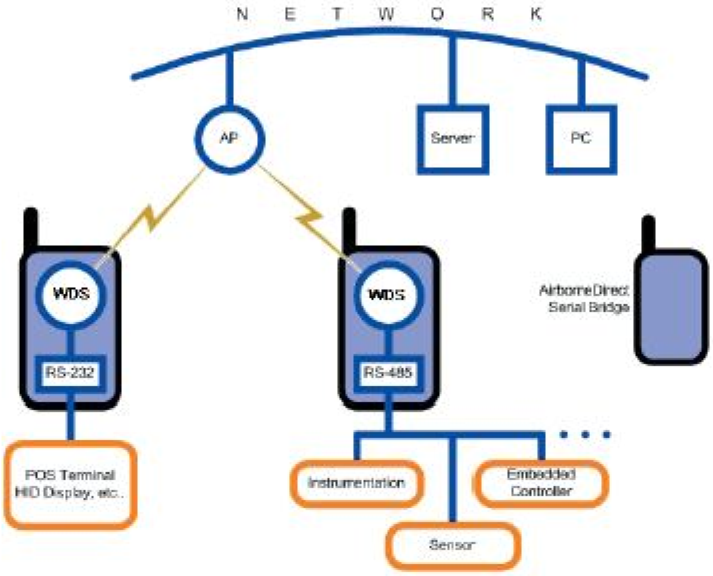


Figure 8.9 Ethernet-to-Wireless Bridge

After a long search, we chose the Airborne wireless-to-Ethernet bridge. AirborneDirect is a family of fully integrated 802.11 wireless LAN device server products designed to provide wireless LAN and Internet connectivity to transportation, medical, warehouse logistics, POS, industrial, military and scientific applications.

The highly integrated hardware and software enables plug-and-play capability. This significantly reduces the complexity of wireless system deployment and network connectivity. Integrating AirborneDirect with existing OEM platforms can significantly enhance the product's value and functionality giving the OEM a competitive advantage.

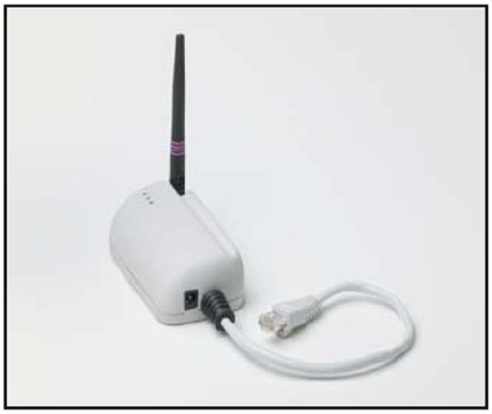


Figure 8.10 Airborne Ethernet-to-Wireless Bridge used in our project.

AirborneDirect™ is a fully integrated, 802.11 wireless Local Area Network (LAN) connectivity device designed to provide wireless LAN and Internet connectivity in industrial, scientific, medical, and transportation applications where an existing communications interface already exists. The AirborneDirect™ Ethernet Bridge is well suited to the following applications:

- Point-of-sale devices.
- Medical equipment.
- Manufacturing machinery.
- Bar-code readers.
- Time clocks.
- Scales.
- Data-collection devices.
- Vehicle Diagnostics.
- Telematics.

The AirborneDirect™ Ethernet Bridge provides true plug-and-play wireless connectivity. By delivering convenient, easy-to-deploy wireless network connectivity, the Bridge significantly reduces the complexities of wireless system deployment and network implementation. At the same time, users can move equipment without the cost and time associated with wired network drops and environment restrictions. This provides flexibility for seasonal demands, line and staffing changes, and more.

The AirborneDirect™ Ethernet Bridge provides a bridge between the 802.11 wireless LAN and any Ethernet-ready device with an RJ-45 connector. It acts transparently between the device and a wireless LAN. By integrating AirborneDirect™ into existing and legacy platforms, OEMs can significantly enhance their products by delivering increased value and functionality to their entire customer base.

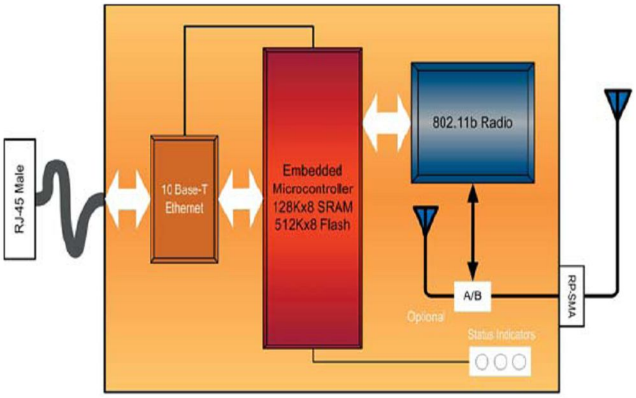
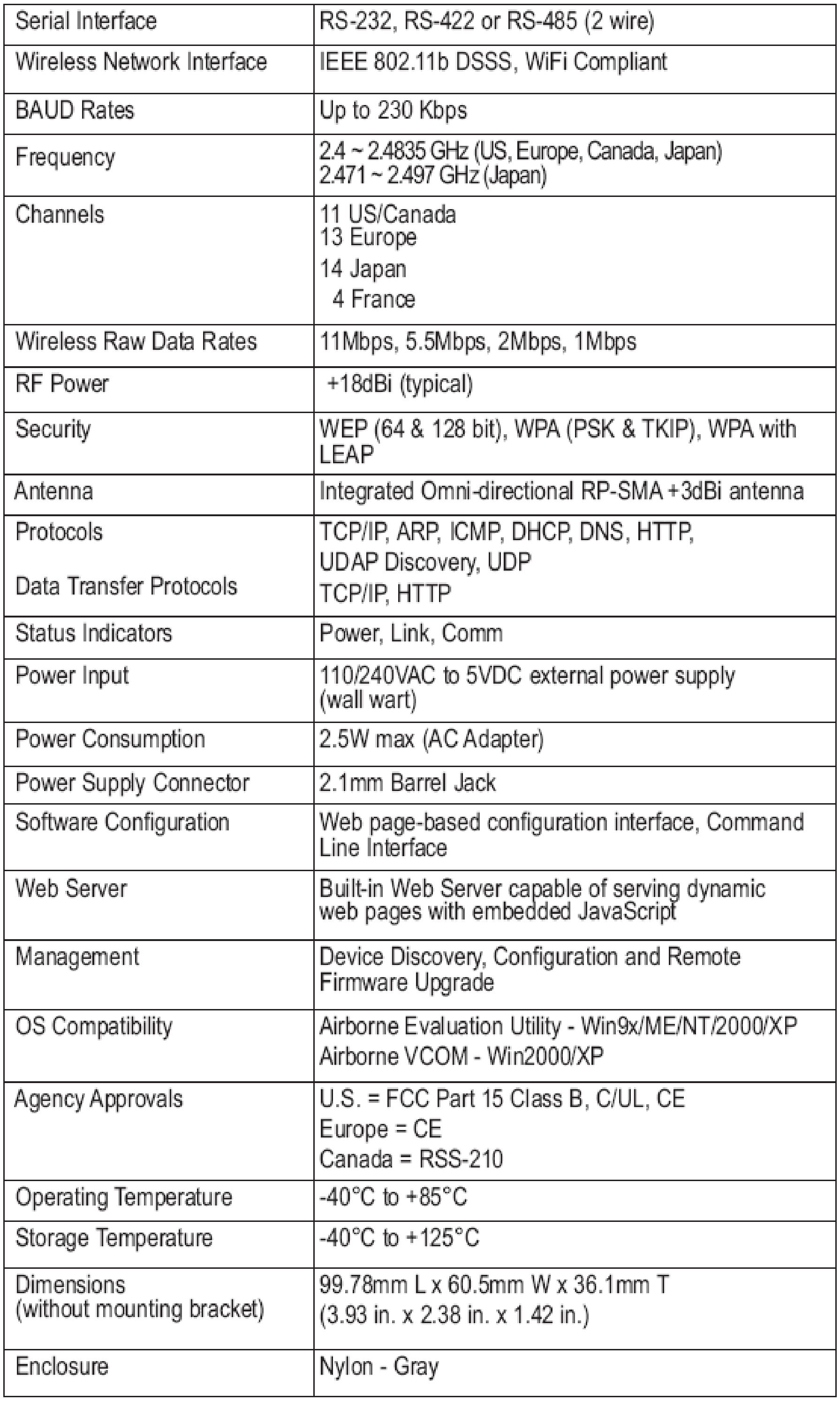


Figure 8.11 Block diagram of Airborne Ethernet-to-Wireless Bridge.



Serial Interface	RS-232, RS-422 or RS-485 (2 wire)
Wireless Network Interface	IEEE 802.11b DSSS, WiFi Compliant
BAUD Rates	Up to 230 Kbps
Frequency	2.4 ~ 2.4835 GHz (US, Europe, Canada, Japan) 2.471 ~ 2.497 GHz (Japan)
Channels	11 US/Canada 13 Europe 14 Japan 4 France
Wireless Raw Data Rates	11Mbps, 5.5Mbps, 2Mbps, 1Mbps
RF Power	+18dBi (typical)
Security	WEP (64 & 128 bit), WPA (PSK & TKIP), WPA with LEAP
Antenna	Integrated Omni-directional RP-SMA +3dBi antenna
Protocols Data Transfer Protocols	TCP/IP, ARP, ICMP, DHCP, DNS, HTTP, UDAP Discovery, UDP TCP/IP, HTTP
Status Indicators	Power, Link, Comm
Power Input	110/240VAC to 5VDC external power supply (wall wart)
Power Consumption	2.5W max (AC Adapter)
Power Supply Connector	2.1mm Barrel Jack
Software Configuration	Web page-based configuration interface, Command Line Interface
Web Server	Built-in Web Server capable of serving dynamic web pages with embedded JavaScript
Management	Device Discovery, Configuration and Remote Firmware Upgrade
OS Compatibility	Airborne Evaluation Utility - Win9x/ME/NT/2000/XP Airborne VCOM - Win2000/XP

Agency Approvals	U.S. = FCC Part 15 Class B, C/UL, CE
	Europe = CE
	Canada = RSS-210

Operating Temperature	-40°C to +85°C
Storage Temperature	-40°C to +125°C
Dimensions (without mounting bracket)	99.78mm L x 60.5mm W x 36.1mm T (3.93 in. x 2.38 in. x 1.42 in.)
Enclosure	Nylon - Gray

Table 8.4 Specifications of the Airborne bridge.

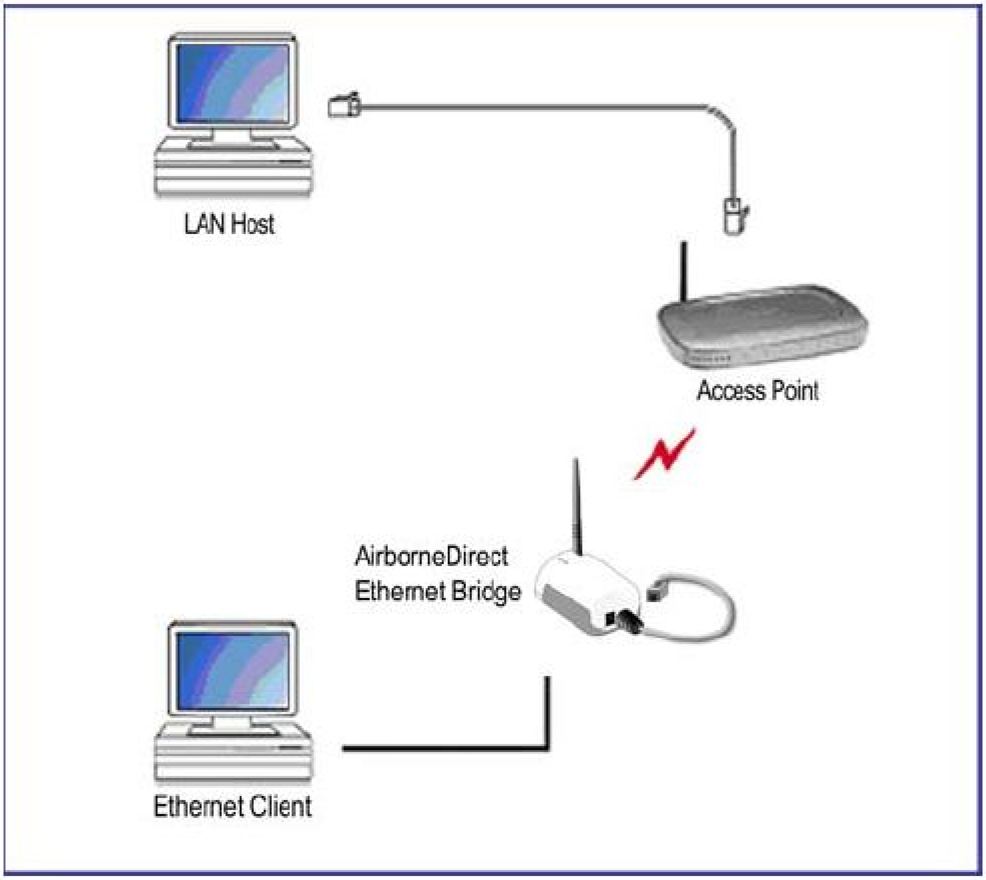


Figure 8.12 Basic Application Involving a LAN Host and Ethernet Client

Referring to the above figure, a LAN host connects to an Ethernet client by setting the destination IP of the Ethernet client rather than the IP of the bridge itself. The IP of the bridge itself is only used to configure it.

This bridge gave us two choices of operations: ad-hoc and infrastructure (where we can only connect to it via a wireless access point). We had chosen infrastructure mode due to the reasons mentioned before.