Dr. Farallon’s Guide
to Wireless LAN Connectivity

Cost-effective and flexible client access to email, Internet, printers and more without wires!
# Table of Contents

- **Introduction** ........................................... 2
- **Wireless LAN Applications** ................................ 3
  - Infrastructure Wireless LAN Networking ................. 4
  - Peer-to-Peer Wireless LAN Networking .................. 4
- **Wireless LAN Technology Defined** .......................... 5
  - IEEE 802.11 Wireless Standard .............................. 5
  - DSSS (Direct Sequence Spread Spectrum) .................. 5
  - 2.4GHz Frequency Band with 14 Channels Allocated ...... 5
  - Access Points ........................................... 6
  - “Soft” Access Point ..................................... 7
  - Data Transmission Modes and Throughput ................. 7
  - Operating Range ......................................... 8
  - Number of Users Supported ............................... 8
  - Wireless Management and Security ....................... 8
- **The Benefits of IEEE 802.11 DSSS Wireless Technology** ........ 9
  - Flexibility and Mobility ................................ 9
  - Affordability .......................................... 9
  - Performance and Reliability ............................. 9
  - Interoperability and Scalability ......................... 9
- **Creating Wireless Computer Labs** .......................... 10
  - Ad Hoc Peer-to-Peer Wireless Lab ......................... 10
  - Small Wireless Lab with Apple's AirPort .................. 11
- **Wireless Integration with an Ethernet LAN** ................. 12
- **Designing a Wireless Campus Area Network** ................ 13
- **Wireless in your Home or Small Office** .................... 14

Dr. Farallon & How to Contact Us
Introduction

Imagine not being tied to your desk for access to LAN (local area network) resources such as the Internet connection, email server, database files, printers and more. Now imagine not pulling wires through brick walls and across campus to gain access to these very same LAN services. Wireless LAN technology allows for client computer communication without wires to access the local network services.

Wireless technology frees users from the physical limitations of a wired connection for communications. Wireless devices communicate without wires to a communications network, for example, a cordless phone in your home communicates wirelessly to its recharge/power station which is physically connected to the wired telephone network.

This white paper identifies the key wireless LAN applications and defines the components of the industry leading 802.11 DSSS wireless LAN technology. The second half of this document provides real-world examples of wireless LAN implementations from creating a computer lab to implementing a wireless campus area network and using wireless at home.

NOTE: Wireless LAN vs. Wireless WAN

Wireless LAN technology should not be confused with cellular or radio modems used for wireless WAN connectivity to the Internet. Wireless LAN technology provides “in-building” connectivity to a wired network's Internet connection.
Wireless LAN Applications

Wireless LAN applications offer computer users the reliable and high performance connectivity of wired LANs with the added flexibility, mobility and affordability of wireless. Wireless LAN connectivity is defined as client access to network resources such as email, the Internet, file servers, printers and database applications without needing to physically connect to the local area network.

Wireless LAN networking is ideal for school and business environments:

1. Where pulling network wiring is costly and difficult, if not impossible, such as in:
   • large open spaces like auditoriums and conference halls
   • campus environments with multiple buildings
   • multi-use spaces that require flexible configuration
   • buildings where materials such as brick, concrete or asbestos are prevalent.

   With wireless networking there is no need to pull extra wires, stretch cabling across a large space, break through walls or dig trenches to the next building.

2. Where temporary LANs need to be quickly set-up, configured and potentially moved, such as for:
   • ad-hoc computer labs in unwired, multi-use spaces
   • offices used by visitors or personnel with no assigned space.

   With wireless technology, a LAN connection or temporary network can be established anywhere within an office, building or campus environment.

3. Where mobile computer users require access to fixed local network resources, internet services, libraries and data centers from several locations. For example:
   • workers whose job requires them to spend time in various locations, including non-wired rooms
   • students and staff who go from classroom-to-classroom, building-to-building and outdoors.

   With wireless, local area network resources can be available to mobile computer users for access to email, the Internet connection, library databases and more.
Infrastructure Wireless LAN Networking

Through the deployment of devices called access points or base stations, wireless LAN technology can be used to extend the reach of a wired network. An access point typically has an Ethernet port for connection to the wired network, and an antenna for wireless communication. Software is built-in to "bridge" the wireless and wired networks. By communicating wirelessly via an access point, computer users can take advantage of wired network services with the flexibility of wireless.

Peer-to-Peer Wireless LAN Networking

Without an access point, users can build wireless ad hoc peer-to-peer networks for anytime, anywhere direct file sharing between two or more wireless-equipped computers.
Wireless LAN Technology Defined

IEEE 802.11 Wireless Standard

802.11 is the IEEE (Institute of Electrical and Electronics Engineers) standard for wireless networking - sending Ethernet data packets through the air. The standard allows for wireless integration with wired IEEE 802.3 Ethernet networks using devices called access points or base stations. This means the IEEE 802.11 wireless standard supports all standard Ethernet network protocols including TCP/IP, AppleTalk, NetBEUI and IPX.

DSSS (Direct Sequence Spread Spectrum)

The 802.11 wireless standard currently includes 3 different types of radio technologies; diffused infra-red (DFIR), Frequency Hopped Spread Spectrum (FHSS) and DSSS (Direct Sequence Spread Spectrum).

802.11 DSSS is the leading wireless technology supported by Apple with AirPort as well as 3Com, Farallon, Lucent, Nokia, Nortel and others. DSSS uses a fixed channel for communication. A DSSS wireless device needs to be on the same channel as the access point to be able to communicate with it. Because fixed channels are used, better performance can be achieved by configuring multiple access points on different channels. This way users will not be competing for the same bandwidth all the time through a single access point.

NOTE: The 802.11 wireless standard does not support interoperability amongst systems of different types. Therefore 802.11 DSSS solutions are NOT compatible with 802.11 FHSS, 802.11 DFIR or other wireless standard solutions such as HomeRF.

2.4GHz Frequency Band with 14 Channels Allocated

802.11 DSSS works in the 2.4GHz frequency band which does not require a license in most countries and provides higher performance than lower frequencies. Fourteen 2.4GHz channels are allocated for worldwide use; 1-11 for USA and Canada, 1-13 for Europe, 12-13 for Spain, 10-13 for France, and 1-14 for Japan.

**DSSS PHY FREQUENCY CHANNEL PLAN**

<table>
<thead>
<tr>
<th>Channel</th>
<th>Frequency</th>
<th>FCC</th>
<th>IC</th>
<th>ETSI</th>
<th>Spain</th>
<th>France</th>
<th>MKK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>USA</td>
<td>Canada</td>
<td>Europe</td>
<td>Spain</td>
<td>France</td>
<td>Japan</td>
</tr>
<tr>
<td>1</td>
<td>2412 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2417 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2422 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2427 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>2432 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>2437 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2442 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>2447 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>2452 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>2457 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>11</td>
<td>2462 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>12</td>
<td>2467 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>13</td>
<td>2472 Mhz</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>14</td>
<td>2484 Mhz</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Each wireless channel creates a separate network, so devices using channel 1 are not on the same network as those on channel 7. In order to avoid interference from adjacent channel traffic when setting up several wireless networks, a 5 to 6 channel spread is recommended.

This configuration allows for the radio waves to overlap without effecting overall bandwidth to the wireless client computers. A well developed client driver is what provides portable users the ability to move between access points transparently.

Access Points

An access point, or base station, is a radio receiver and transmitter that connects to your wired Ethernet network. Through these devices wireless nodes, such as a Macintosh PowerBooks or PC notebooks equipped with a Farallon SkyLINE Wireless PC Card, have access to wired LAN network services like email, Internet, printers and more. Operating range, management capabilities, wireless network security and number of users supported are determined by the capabilities of the access point.
“Soft” Access Point

As an alternative to deploying an access point for wireless connectivity to a wired Ethernet network, a computer that is physically connected to an Ethernet network, outfitted with a wireless card such as SkyLINE, and running a software routing solution such as Vicomsoft Internet Gateway (www.vicomsoft.com), can act as the gateway between the wired network and the wireless network.

Data Transmission Modes and Throughput

There are two modes, encapsulation and translation, for transmitting data over a wireless network. Encapsulation mode encloses the 802.3 Ethernet packets inside 802.11 frames for transmission through the air, where as translation mode converts 802.3 Ethernet packets into 802.11 packets for transmission. Recently translation has emerged as the defacto standard, but support for encapsulation as well ensures maximum flexibility in networks where both addressing modes may be used.

The 802.11 DSSS wireless standard provides for data throughput of 2M bps up to 11M bps. Data transmission speeds can be affected by a variety of factors including number of users on the network, individual processor speeds, application resource requirements, etc. Compared to an Internet connection, 2M b 802.11 DSSS is comparable to a T1 line of 1.5444M bps. This means your wireless network will not be a bottleneck to Internet applications such as email and web access.
Operating Range

Factors that affect the operating range of any wireless device include the strength of the access point, the number of walls inside a building, the construction materials used within a building (concrete vs. steel vs. wood) and the data transmission speed.

Most access point manufacturers offer enhanced antennas for increased range. Manufacturers recommend that access points be deployed 150ft (50m) apart to ensure full coverage and maximum data throughput rates for roaming computer users. Additionally, a step down in data transmission speed will increase the operating range. So, a wireless client communicating at 2M bps will have better range than a client at 11M bps.

Access points can be used to extend the range of a wireless network even in situations where there is no need to connect back to a wired Ethernet network. By deploying an access point as a “wireless hub” the distance between two remote computers can be extended up to 300 feet (150 feet from each computer to the access point) depending on the configuration of the building and the location of the access point.

Number of Users Supported

Most access point manufacturers support anywhere from 10 to 50 simultaneous users per channel while some go as low as 5 and others as high as 100. The same principles that apply to sharing wired bandwidth using a hub apply to sharing wireless bandwidth through an access point. The data bandwidth of a single access point is shared with all the wireless users connected to that access point. So, just like 5 computer users connected through a standard Ethernet hub share the bandwidth, 5 wireless users connected through an access point share the bandwidth.

Wireless Management and Security

Certain wireless client solutions provide utilities to monitor the strength of the signal and data throughput speeds. For example, the Farallon SkyLINE Control Panel shows wireless computing users real-time network statistics. Additional wireless network management capabilities are incorporated into the access point and depend on the manufacturer and model. Management interfaces include Windows 95/98, Windows NT, Mac OS with Apple's AirPort, http, FTP, Telnet, and SNMP.

As with wired networks, the first line of security defense are the User IDs and passwords in the Operating System of client computers and servers. Additional security varies from one access point to another. Many access point manufacturers allow network administrators to limit the access point connections by creating a table of wireless client hardware (MAC-Media Access Control) addresses. Some access points include software encryption or WEP (Wired Equivalent Protection) 40-bit encryption.
The Benefits of IEEE 802.11 DSSS Wireless Technology

Flexibility and Mobility

Wireless LANs offer the ultimate in flexibility and mobility when it comes to networking. In addition to being able to build ad hoc labs, wireless LAN networking is key for roaming computer users who need access to services like email, the Internet and printers from various locations. Roaming is the ability for a wireless user to move from room to room, or even building to building on a campus, and not lose their connection with the network. Although roaming is not specifically addressed in the 802.11 DSSS wireless standard, it is one of the great benefits of using laptop computer equipped with wireless.

Affordability

Wireless LAN networking avoids the high costs of pulling cable and installing network drops. Additionally, wireless networking is much more cost-effective when it comes to frequent computing resource relocation and reconfiguration needs.

Interoperability and Scalability

802.11 DSSS is the industry standard supported by Farallon along with leading companies such as Apple, 3Com, Lucent, Nokia, Nortel and others. The 802.11 wireless standard ensures backwards compatibility. This means 802.11 DSSS solutions of different data transmission rates will work together. Therefore, when the emerging 11Mb 802.11b DSSS solutions become available, they will interoperate with the currently shipping 2Mb 802.11 DSSS solutions.

For easy integration with a wired Ethernet network, 802.11 DSSS supports all standard Ethernet network protocols including TCP/IP, AppleTalk, NetBEUI and IPX. Additionally, the translation and encapsulation modes allow for the conversion of 802.3 packets from a wired Ethernet network to 802.11 packets for wireless transmission and visa versa.
Creating Wireless Computer Labs

Wireless LANs are ideal for creating anytime, anywhere computer labs. Multi-purpose computers can easily be moved, and a small network can quickly be set-up in multi-purpose spaces that may not be conveniently wired. There are two configurations for setting-up a wireless computer lab; peer-to-peer or by using an access point, such as the Apple Airport, to act as a wireless hub.

Ad Hoc Peer-to-Peer Wireless Lab

A peer-to-peer wireless lab allows the wireless nodes to share files directly without using an access point. Each wireless-equipped node is simply set to ad hoc mode for communication.

Note: In order for all computers to communicate wirelessly together, they need to all follow the same wireless standard. For example, each node would need to be equipped with 802.11 DSSS solutions such as Farallon’s SkyLINE Wireless PC Card for Macintosh PowerBooks or PC notebooks. An Apple iBook would need to be equipped with the 802.11 DSSS AirPort wireless option.
Small Wireless Lab with Apple’s AirPort

A small wireless lab can also easily be set-up with an access point such as the Apple AirPort. Instead of communicating directly with each other as in the previous peer-to-peer example, the wireless nodes all connect wirelessly through the access point. The access point acts as a wireless hub, and since it is equipped with an Ethernet port, a wired connection to a printer or Ethernet drop in the room can also be made.

If Internet access is needed and connection to the network backbone is not convenient or possible, the Apple AirPort base station’s 56K modem can be used for direct wireless client access to the Internet through the AirPort modem.

Note: Since Apple’s AirPort base station follows the 802.11 DSSS wireless specification, the lab computers all need to be equipped with 802.11 DSSS solutions such as Farallon’s SkyLINE Wireless PC Card for Macintosh PowerBooks or PC notebooks. Apple iBooks would need to be equipped with the AirPort wireless option.
Wireless Integration with an Ethernet LAN

As described earlier, wireless nodes gain access to wired Ethernet network services through Access Points or Base Stations. The access point and wireless nodes must all be using the same wireless standard in order to interoperate on the same network. Hence, deploying the leading 802.11 DSSS wireless LAN standard requires an 802.11 DSSS access point to be connected to your wired Ethernet LAN and the use of 802.11 DSSS-equipped wireless nodes.

Just like other Ethernet devices such as desktops, servers, printers, routers, hubs and switches, an access point comes with Ethernet on board for a direct physical connection to the wired network. Wireless communication is conducted through a radio antenna built into the access point.

As long as the access point can be plugged in to the wired network and is positioned to get maximum area coverage for wireless nodes (up high, with as little obstruction as possible), it can be located in a room, network closet, common area, etc. Every access point offers its own set of features and the operating range, number of users supported, security features, and management capabilities all vary from one model to the next. Once the access point is set-up on the Ethernet LAN, all wireless-equipped nodes will have access to the LAN resources, just like the wired nodes.
Designing a Wireless Campus Area Network

In the previous section we explained how to integrate a wireless network with a wired Ethernet LAN. On a campus area network, where wireless clients are likely to roam around campus and between buildings, multiple access points can be deployed to provide campus area wireless access to the Ethernet LAN. For example, a university may want to provide wireless access to students and faculty from multiple locations on campus. In order to accomplish this, the university would deploy an access point in each of the locations from which they want to provide wireless access to users.

As mentioned before, access point manufacturers recommend the implementation of an access point for every 150ft of range required for wireless network access. Each access point operates on a channel, and wireless devices using channel 1 are on a separate network from wireless devices on channel 7. In order to avoid interference from adjacent channel traffic when setting-up separate wireless networks, a 5 to 6 channel spread is recommended.

Wireless nodes have the capability to connect to one access point or another, but since the 802.11 DSSS specification for wireless networking does not specifically address roaming, there are differences in how wireless client solutions handle multiple access points and roaming between them. Some wireless client solutions require the user to reconfigure the wireless node every time a network connection is lost and connection to a different access point is required to regain network access. Other wireless client solutions, such as Farallon’s SkyLINE Wireless PC Card, can be configured to automatically connect to an access point within range.

Implementations

How Farallon’s SkyLINE Handles Roaming

Farallon has made roaming much easier. On both the MacOS and Windows sides, the Farallon SkyLINE Wireless PC Card simplifies roaming provided all the access points have the same name. For example, the user enters this name, WirelessAP for instance, in the access point configuration screen. When a user is in one location connected wirelessly to an access point called WirelessAP and moves to a new location, SkyLINE will automatically connect to a new access point called WirelessAP that is within range.

Macintosh users have a second option called “select the best.” When using this option, SkyLINE will connect to the nearest, strongest access point it finds. When the user moves out of range of that access point, SkyLINE will go into hunt mode and find a new access point, no matter what the name. This feature also allows the user to roam between access points from different vendors.

\[ AP = \text{Access Point} \]
Wireless in your Home or Small Office

Similarly to a small wireless computer lab in a school or business environment, a small wireless network can be set-up in your home. As explained, an ad hoc peer-to-peer wireless network can be created for file sharing, but in the home you would most likely also want to share printers, an Internet connection and other network devices or services.

Apple’s AirPort base station is ideal for setting-up a small network at home to share a single Internet connection, play multi-user games, share printers, files and more. With the addition of a small 10Base-T hub, such as a Farallon Starlet, the AirPort Ethernet connection can be expanded to connect printers, desktop computers and other wired network devices.

Note: Since Apple’s AirPort base station follows the 802.11 DSSS wireless specification, any wireless node in your home must be equipped with an 802.11 DSSS solution such as Farallon’s SkyLINE Wireless PC Card for Macintosh PowerBooks or PC notebooks. Apple iBooks would need to be equipped with the AirPort wireless option.
Dr. Farallon's Network Clinic
FREE Personal Network Consultation - No Matter What Your Budget

The Dr. Farallon Network Clinic offers free advice to anyone seeking information on how to create, expand or improve their network. Dr. Farallon network specialists are experienced technicians who can help you with planning for network growth, budgeting for network improvements and optimizing network performance.

Contact Dr. Farallon Today!
Call: 1-800-613-4954
Visit: www.farallon.com/dr.farallon/