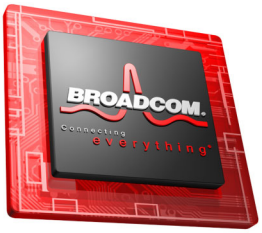
White Paper

Practical Strategies for Deploying WiFi® Clients

Wireless-WP101-R

This white paper offers practical strategies to help you choose wireless technology that will future-proof client network devices today. Armed with this information, you'll be ready to take advantage of infrastructure that is added or upgraded in the future.

October 19, 2003



Introduction

Though not yet ubiquitous, wireless networking is proliferating rapidly. Hospitals, retail shops and warehouses began using the technology several years ago for targeted applications. Once new standards enabled higher-speed networks, a few bold enterprises began deploying the technology in 2000 to connect office workers. After seeing improvements in standards-based wireless networking security, large-scale enterprises are starting to implement the technology more broadly to improve connectivity and productivity — and small- and medium-sized businesses have followed suit.

The benefits of the technology over conventional wired LANs are as clear as they are numerous. For one, wireless technology eliminates the cabling headaches of setting up a network. And with wirelessly enabled mobile computers, workers can remain connected to the network, whether in a conference room, in the break room or in an impromptu team meeting. From home networks to commercial public-access points or hot spots, it's getting easier all the time to extend the office LAN to wherever your clients might be doing business.

Even if you're still contemplating deployment of a wireless network, chances are increasing by the day that notebook computer purchases will include wireless LAN capabilities. Major notebook PC manufacturers have shifted from offering wireless LAN known as Wi-Fi technology as an add-in PC Card option to including Wi-Fi capabilities in mobile PCs as a standard feature. In fact, recent data indicates more than 40 percent of their notebooks include built-in Wi-Fi capability[1] – and that percentage continues to climb.

Wireless LAN technology is expanding beyond the domain of notebooks to include office peripherals and mobile devices like PDAs. Printers and scanners are incorporating Wi-Fi capabilities, as are handheld computers, so business professionals can check e-mail, synchronize calendars, print on the fly and access the Internet while on the go. Manufacturers of cell phones and business phone systems are planning to add Wi-Fi technology into their products to cut costs with VoIP (Voice over Internet Protocol) technology.

These technology advances mean that today your business is making buying decisions that will affect your wireless LAN investment — regardless of whether you've started deploying the infrastructure for a wireless network. Choosing clients with the right wireless technology can make your wireless networks easier to deploy and configure as well as more productive and secure — whenever you decide to deploy.

[1] Source: TechKnowledge Strategies, Inc. 2003

Choose the Latest Client Technology

The number of wireless LAN devices sold has just about doubled in each of the last four years. The catalysts for this rapid growth included falling prices for access points as well as client hardware built around the IEEE 802.11b wireless networking standard, ratified in July 1999. The standard offers good maximum range, though raw data rates top out at 11 Mbps. That is more than enough bandwidth for single-client consumers who used the connection to pair a notebook computer with an Internet adapter — which happened to be the most common Wi-Fi deployment at the time.

The bandwidth of a wireless network is shared, so 802.11b can bog down (or experience latency) when it performs typical office networking tasks like file sharing between multiple clients. Large file transfers between as few as two 802.11b clients are unacceptably slow for workers who are accustomed to the pace of today's tethered LANs.

There are two technologies available that offer up to five times the raw data rate, or 54 Mbps. One is 802.11g, which operates on the same 2.4 GHz frequency band as 802.11b and is backward-compatible with the older, lower-bandwidth technology. The other alternative, 802.11a, occupies frequencies in the 5 GHz band. It offers less range of coverage than either 802.11b or 802.11g but offers up to 12 nonoverlapping channels, compared to three for 802.11b and 802.11g, so it can handle far more traffic than its 2.4 GHz counterparts.

So when should you choose 802.11a, 802.11b or 802.11g? The combination of short range and capacity for high-volume traffic makes 802.11a well suited for confined, high-traffic areas like crowded conference rooms and high-bandwidth applications like streaming media. The longer range for 802.11g is more appropriate for larger areas and, because of its compatibility with 802.11b, will function at hot spots, many of which are outfitted with the older standard.

Ratified in June 2003, 802.11g is currently the fastest-growing wireless LAN technology[2] because of its attractive price-performance ratio. That said, computer makers are increasingly offering notebooks with built-in, dual-band 802.11a/g capability — an option that might prove to be the best future-proof option for today's notebook PC purchases, as they will be ready for any direction in which your network evolves.

At this stage in the market, you would be wise to avoid mobile computers with only integrated 802.11b Wi-Fi, such as the wireless component inside Centrino™-equipped notebooks shipping throughout 2003. With built-in options that are faster and higher-capacity — as well as backward-compatible with the older standard — it

[2] Source: TechKnowledge Strategies, Inc. 2003

is hard to justify capping your developing wireless network at data rates that modern Ethernet networks surpassed years ago.

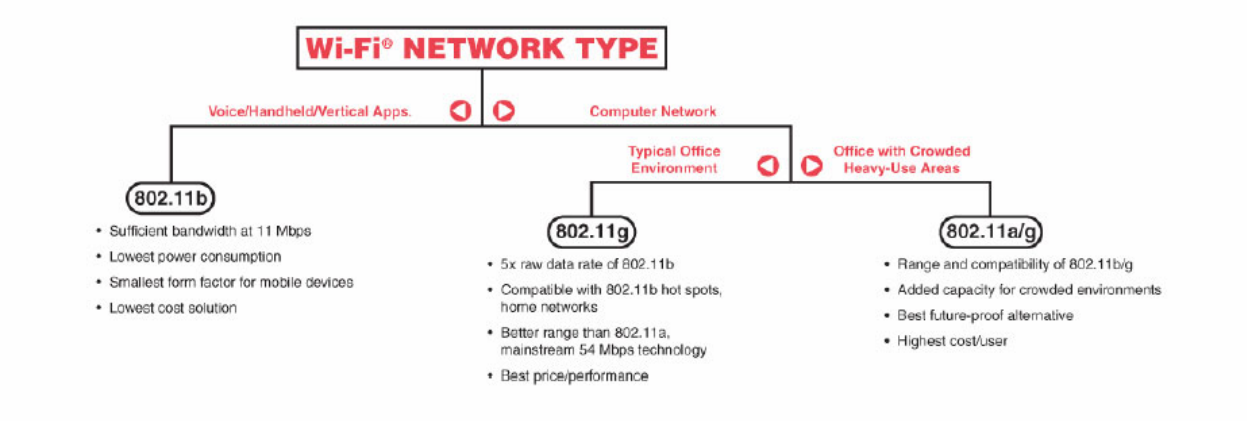


Figure 1: Wi-Fi Client Technology Decision Tree

This certainly does not mean that 802.11b will disappear altogether. It provides connectivity with good coverage at an attractive price. Because 802.11b solutions are the least technically complex Wi-Fi® solutions, manufacturers can produce 802.11b solutions that are highly integrated, consume less power and are less expensive than solutions based on the higher data-rate standards. As a result, 802.11b is ideal for pocket-size mobile devices like phones and PDAs that require low-bandwidth connectivity for applications like voice, e-mail, text messaging and calendar synchronization.

Keep in mind, however, that 802.11b implementations do not automatically consume less power than 802.11g offerings. In fact, some older 802.11b offerings — such as the one bundled inside Centrino computers — actually consume more power than some newer 802.11g chipsets.

Stick with Standards

Performance matters, as already discussed. But not at all costs.

In particular, it is wise to avoid non-standard schemes that promise raw data rates beyond 54 Mbps. For example, the higher data-rate solutions currently available cause self-interference in multiple access point environments. While higher data rates may sound enticing, they are unlikely to be worth the added implementation and support costs associated with proprietary solutions, and may actually decrease performance for the standards-compliant nodes in your network. The IEEE is addressing next-generation Wi-Fi® technology — just as it is taking wired Ethernet to gigabit data rates and beyond. In the meantime, however, there is no consistent, interoperable method for extending data rates beyond 54 Mbps.

It is also wise to avoid proprietary schemes that provide extended range. For example, one such technique achieves the extended range by slowing the network below IEEE-specified data rates. So while one user may gain the benefit of extended range connectivity, overall network performance suffers dramatically.

Sticking with IEEE standards is critical for potential device interoperability, but buyers should seek Wi-Fi solutions that are certified as interoperable by the Wi-Fi Alliance to guarantee this interoperability. The Wi-Fi Alliance, an independent industry organization, tests all Wi-Fi products at a third-party facility to weed out incompatibilities between access points and client hardware built around competitive Wi-Fi chipsets. Many wireless products prominently feature the Wi-Fi CERTIFIED™ logo, and the most complete list of Wi-Fi CERTIFIED™ products can be found on the Wi-Fi Alliance Web site (www.Wi-Fi.org).

Pay Attention to Performance

If performance is of primary concern, you should be aware that not all wireless LAN solutions are created equal — even within the confines of the standards. Indeed, some chipsets offer enhanced performance features built into the standards. As a result, careful shopping will yield better-performing networks — but without all the support headaches of proprietary solutions.

One such example is a technique called frame bursting. Frame bursting improves performance by eliminating some overhead traffic, thereby leaving more of the available bandwidth for data. Frame bursting is an extension of a feature in an early version of the 802.11 specification, and it is featured in drafts of the upcoming 802.11e specification to improve network quality of service. Unlike proprietary techniques, open implementations of frame bursting improve performance for a wide range of network configurations — regardless of whether other network nodes implement the feature.

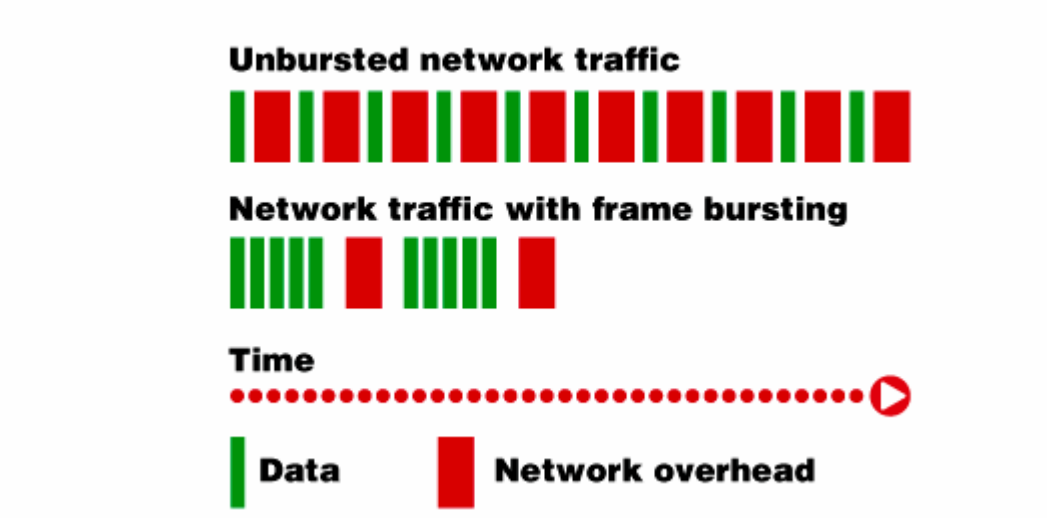


Figure 2: Improved Efficiency with Frame Bursting.

Throughput rates are one aspect of Wi-Fi performance that should be considered. Power consumption is another important decision criterion for a networking technology designed for battery-powered hardware like notebook computers. Some Wi-Fi chipsets consume less power in performance mode while transmitting and receiving data. Some chipsets offer better power-saving modes, so they are more

adept at ratcheting down power demands while waiting to detect network activity. Obviously, chipsets that offer the lowest power consumption in both performance and power-saving modes will lead to the best battery life for wirelessly connected mobile devices. Another area requiring close attention is the range and robust quality of the Wi-Fi signal, because it will differ from implementation to implementation. Simply put, robustness is the ability of the Wi-Fi to maintain higher data rates at longer distances. As is defined by the standards, the network maintains a given data rate as long as the access point and client can preserve a strong data connection. Once they can't, they dip down to a lower data rate and try again. So the closer the clients are to the access point, the more likely they will be able to communicate at the network's maximum raw data rate.

Careful equipment selection will prove most beneficial if you choose Wi-Fi hardware with a well-designed radio, an adept digital signal processor (DSP) and a capable antenna implementation. Some technical details may be worth probing. For example, many major industry players have opted to use CMOS radios in wireless LANs. The properties of CMOS technology lend themselves better to repeatable, more consistent performance than other chip-manufacturing technologies. The other components in a Wi-Fi chipset are already built into CMOS, so suppliers with CMOS radios are better prepared to integrate the components into a single-chip solution. CMOS radios were first introduced in 2002. Today, CMOS radios are more common than alternative technologies in 54 Mbps products.

Obviously, there are external variables that impact wireless network performance, such as the number of walls between nodes. Interfering radio traffic also challenges the network's ability to sustain higher data rates. Antenna implementations can vary by access point and by computer, and some Wi-Fi chipsets are better equipped than others to maintain higher data rates for longer distances. Look for features — like self-calibration — that are designed to maintain a consistent wireless signal for predictable performance.

One growing cause of interference on 2.4 GHz networks is Bluetooth® — a wireless personal area networking (PAN) technology that is increasingly used to connect telephones with wireless headsets and other peripherals, including notebook computers. Interference immunity is important in general, and some 2.4 GHz Wi-Fi chipsets are better equipped than others to deal with background Bluetooth chatter. When Bluetooth and Wi-Fi radios are built into the same notebook, it is important to choose a solution that incorporates a coexistence interface that ensures the two radios cooperate rather than compete on the 2.4 GHz frequency band.

Understand Security Options

There may be no more important consideration for your developing wireless network than understanding the Wi-Fi security features built into your new mobile clients. Indeed, security concerns have kept businesses from implementing wireless networks until recently, when significant industry-standard enhancements were added.

The initial 802.11 specification provided for the Wired Equivalent Privacy (WEP) algorithm. The foundation for WEP is a secret, 40-bit key that is required to

participate in a given wireless network. Because of technical flaws in its implementation, WEP has proven relatively easy to crack — so it should come as no surprise that technology professionals have resoundingly rejected a full-scale wireless deployment based on WEP.

To provide an acceptable solution, the Wi-Fi Alliance and the 802.11i security task force worked together to create Wi-Fi Protected Access™, or WPA. WPA improves on WEP in two important ways: It implements greatly improved data encryption and adds user authentication. For encryption, WPA employs a technology called temporal key integrity protocol, or TKIP, to offer better security than WEP. TKIP constantly replaces security keys using a complex algorithm while encrypting and adding data-integrity features.

Choose A CMOS Radio Chip

It may sound like arcane advice to seek out Wi-Fi chipsets made with a particular manufacturing technology, but careful attention to this detail will pay dividends. If you do choose a chip set with a CMOS radio, you are likely to end up with wireless clients that are connected more consistently, promote longer battery life - and cost less.

CMOS is by far the most common chip-making process in existence. As a result, it is more widely available, more economical and more reliable than more exotic alternatives. There are properties unique to CMOS that make it better suited for complex, high-speed chips like PC microprocessors as well as circuits for battery-powered applications. Not surprisingly, the digital components in Wi-Fi chipsets are all built in CMOS.

Wi-Fi chipset providers have invested in radio design techniques that produce CMOS radio chips with better repeatability, improved sensitivity and lower power consumption than exotic solutions such as silicon germanium (SiGe) and gallium arsenide (GaAs).

Most believe that all Wi-Fi chipset suppliers will ultimately transition to CMOS radios - they will have to if they hope to build the single-chip Wi-Fi solutions required for pocketsized electronics devices like PDAs and full-featured mobile phones. Until they do, shop carefully and choose Wi-Fi chipsets that already feature CMOS radio chips.

WPA has two modes — WPA-Enterprise and WPA-Personal. In a business setting using WPAEnterprise, authentication begins with the Extensible Authentication Protocol, or EAP, and the 802.1X protocol. This requires the presence of an authenticating RADIUS or similar server. For small businesses and corporate users logging on wirelessly from home, WPA-Personal may be used. WPA-Personal provides a means for the network administrator to dispense with a RADIUS server and just enter authentication keys manually. Deployed properly, this mode simplifies user authentication while maintaining the same strong encryption implemented in the enterprise. For more information on WPA, go to http://www.Wi-Fi .org/OpenSection/pdf/Whitepaper_Wi-Fi _Security4-29-03.pdf.

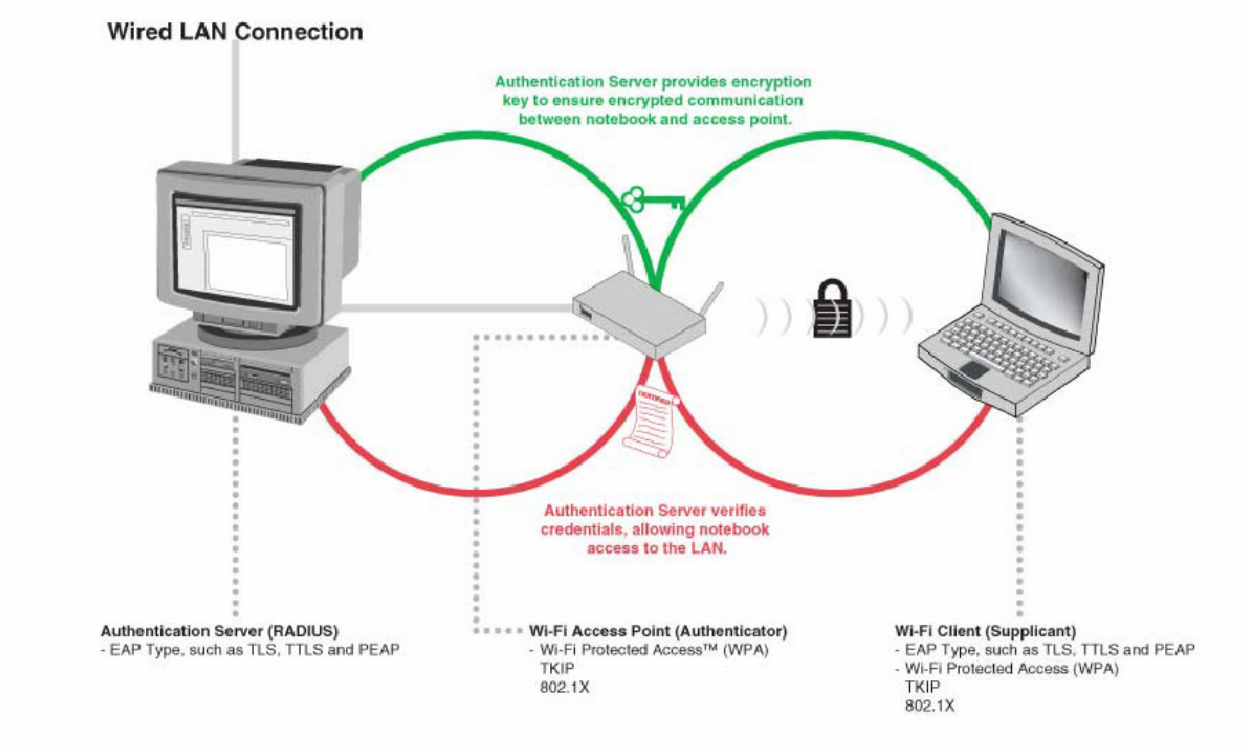


Figure 3: Wi-Fi Protected Access (WPA)

Cisco offers its own flavor of EAP, called LEAP, which is implemented in Cisco access points. Because Cisco hardware is prevalent in the enterprise, some network administrators may want Wi-Fi clients that support LEAP. Cisco is licensing LEAP and other features that leverage a Cisco Wi-Fi infrastructure to suppliers of chipsets for Wi-Fi clients as part of a program it calls Cisco Compatible Extensions (CCX). If you plan to deploy or have deployed Cisco access points, seek out client hardware that is CCX-certified.

WPA is now available in Wi-Fi client hardware. For those who implemented wireless networks before WPA was available, many Wi-Fi chipset vendors offer software or firmware updates to bring older wireless networks in line with the WPA security level.

The next developments in Wi-Fi security are being defined by the 802.11 security task force, the IEEE 802.11i working group. Basically, 802.11i combines WPA with the U.S. government encryption standard, the Advanced Encryption Standard, or AES (http://csrc.nist.gov/CryptoToolkit/aes). WPA is an interim security step. If you are looking to future-proof your wireless clients, look for Wi-Fi chipsets with hardware-based AES that provide the latest functionality without the performance penalty expected from implementations of AES in software.

Plan for Emerging Technologies

Wireless networking is an evolving technology, and new standards are constantly being developed to address the need for additional features, which can be somewhat confusing as you try to future-proof the notebooks you buy today. If they are able, chipset suppliers will add support for new standards to chipsets that are already deployed, which is typically achieved through software upgrades. While software upgrades do bring wireless clients up to par with the latest standards, they do so by adding to the client's workload.

IEEE standards take years to evolve. While standards are never final until the organization ratifies them, in some cases it is clear that features will be included long before the standard is approved. Chipset suppliers can help future-proof today's chipsets by building into the hardware features to be included in upcoming standards. Once the standards are ratified, chipsets with those features built in will shoulder the burden of the new features, offloading the client.

In the previous section, we discussed seeking out wireless clients with support for AES built in as a preferred method of future-proofing for 802.11i. Another way to future-proof clients is to look for hardware with built-in support for features to be included in the upcoming 802.11e standard, such as Quality of Service (QoS) and frame bursting.

Choose Broadcom

Broadcom has a complete portfolio of industry-standard Wi-Fi solutions designed to ensure that your wireless network is state of the art — even if you are deploying only a few nodes. The company is the industry's leading supplier of 54 Mbps wireless LAN chipsets, and its 54g™ solutions are used in more than 95 percent of notebooks[3] that ship with 802.11g, including computers from Apple, Compaq, Dell, eMachines, Fujitsu, Gateway and HP. Broadcom was also the first technology provider to enable dual-band embedded notebook solutions that offer the maximum flexibility by communicating with access points built around the three existing Wi-Fi standards: 802.11a, 802.11b, and 802.11g. And Broadcom's AirForce One™ new single-chip 802.11b offering raises the bar for pocket-size low-power products.

[3] Source: NPD Group, July-August, 2003, U.S. Retail Shipments

Across its AirForce product line, Broadcom's Wi-Fi chipsets offer superior performance, with features like SmartRadio™ that improve range and robust signal reception to maintain the highest data rates possible under various conditions. For example, Broadcom 802.11b and 802.11g chipsets include technology designed to eliminate interference from Bluetooth components, which operate at the same

frequency. And with XpressTM Technology, Broadcom chipsets combine a feature in the original 802.11 specification with a performance feature from the upcoming 802.11e QoS standard to deliver superior industry-standard performance. (For more on Xpress™ Technology, please see www.54g.org/docs/WP2-Xpress-030617.pdf.)

Broadcom has been producing chipsets with CMOS radios since it entered the Wi-Fi market. CMOS radios generally offer more consistent, repeatable performance than alternative technologies. Broadcom's continuous calibration feature — a component of SmartRadio, which extends across the AirForce product line — adds even more reliability by calibrating on the fly. The company's CMOS expertise also enabled the single-chip AirForce One product.

The company's OneDriver™ software was designed to benefit the enterprise. It is a single software-and driver package that covers Broadcom's entire AirForce product line, so you can maintain a stable platform image and easily upgrade all your clients with the latest enhancements whenever you choose to update that image.

WLAN Client Checklist

- Wi-Fi CERTIFIED™ 802.11a
- Wi-Fi CERTIFIED™ 802.11b/g
- WPA and CCX security software
- AES in hardware
- All CMOS technology (including radio)
- High-performance, self-calibrating radio
- Bluetooth co-existence
- Open frame bursting implementation

Broadcom's security portfolio is second to none. Broadcom was one of the first suppliers with chipsets that support WPA, and was also one of the first to achieve CCX certification from Cisco. Broadcom also includes hardware AES support in advance of the upcoming 802.11i specification.

And Broadcom's new single-chip 802.11b offering isn't the only one in the portfolio to boast low-power advantages. In fact, the company's 802.11g chipsets are both five times faster and consume less power than the 802.11b hardware bundled into Centrino notebooks.

All things considered, the best way to future-proof your wireless network — whether you are deploying it yet or not — is to seek out mobile computers and other clients with built-in Broadcom chipsets. Broadcom technology is designed so

that the devices you own today — and those you add tomorrow — will connect reliably, seamlessly and securely. Broadcom Wi-Fi technology is available from these leading manufacturers: Apple, Belkin, Buffalo, Compaq, Dell, eMachines, Fujitsu, Gateway, HP, Linksys/Cisco, Microsoft and Motorola.

Phone: 949-450-8700
Fax: 949-450-8710
E-mail: info@broadcom.com
Web: www.broadcom.com

BROADCOM CORPORATION
16215 Alton Parkway, P.O. Box 57013
Irvine, California 92619-7013

Wireless-WP101-R 04/12/05