

Riding the Wireless Wave

Challenges faced by SMBs in an Increasingly Unwired Landscape

Introduction

The wireless broadband market in Singapore is still in its very nascent stages. Mid-June 2005 saw licenses being awarded to 6 service providers¹ to offer wireless broadband access (WBA) services. Operators have since been quick to roll out fixed wireless products targeted at supplying broadband access to fixed locations or hotspots. The WBA market is expected to evolve fairly quickly, with mobile broadband services offerings expected to be made readily available by the end of 2007 with pre-WiMax trials already underway.

The implications of this development are two-fold. On the plus side, applications such as VoIP and video streaming, will become commonplace for the road warrior or fieldworker. On the other hand, users will have to deal with issues such as security and compatibility.

This article provides a brief overview of the wireless broadband landscape and looks at ways in which users, specifically SMBs, can benefit from this technology. It then explores the various challenges faced by SMBs in their adoption of wireless broadband services and provides advice on how SMBs can deal with issues related to wireless security.




Challenges faced by SMBs

Over the years, IT has come to be increasingly regarded as a tool that can increase business productivity and efficiency. IT *does* matter, and more so, for organizations seeking to remain competitive in an increasingly globalized economy.


Figure 1 illustrates the different roles that IT play as SMBs mature over time. Essentially, there are 3 waves of IT adoption. On an elementary level, an SMB would purchase basic IT infrastructure including PCs, anti-virus software and internet access. As the SMB grows in maturity in its IT usage, it would look to invest in IT to help connect the enterprise. In the third wave, it is expected that the SMB will leverage the network to extend the enterprise through effective use of applications such as CRM/ERM/SCM and IP-based networks.

¹ inter-Touch Holdings, MobileOne, Pacific Internet, Qala Singapore, Singapore Telecom Mobile and StarHub

Figure 1: Evolution of the SMBs: 3 Waves of IT Adoption

								
Wave I		Wave II		Mega Wave III				
Building The Basic Infrastructure		Connecting The Enterprise		Extending The Enterprise (Leveraging the Network)				
	SB	MB	SB	MB	SB	MB		
PC *	44%	100%	LAN	32%	74%	WAN	4%	34%
Internet	81%	98%	High-Speed	58%	85%	VPN	12%	44%
Anti-Virus	60%	84%	e-Commerce Web Site	10%	22%	SAN/NAS	3%	26%
Basic Web Site	32%	76%	WLAN	8%	23%	CRM	1%	8%
			Desktop Firewall	35%	39%	ERP/SCM	4%	17%
			Network Firewall	35%	58%	IP Centrex	0.2%	1%
						IP PBX	1%	8%

% of PC Small and Medium Businesses
 * % of All Small and Medium Businesses


 Evolving Distribution, Ecosystem Partners, Business Processes, Security and Service/Support Needs
 (Data Above Shows 2005 Penetration Among WW SMBs)

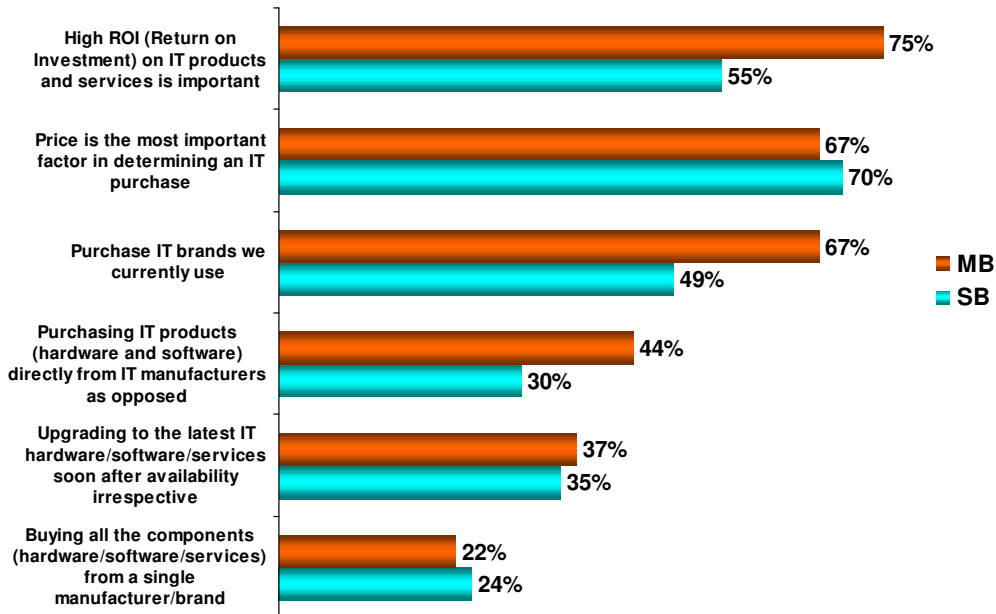
Source: AMI-Partners, 2006

Notes: Based on global SMB research

Like their counterparts in the rest of the region, SMBs in Singapore face an uphill task in understanding how to harness technology to increase productivity. Like most SMBs, these organizations also face challenges of managing costs and increasing profitability.

Figure 2 reflects the attitudes of SMBs towards technology. Not surprisingly, price remains a key concern for decision makers, particularly with small businesses (SBs) while medium-sized businesses (MBs) are more concerned with obtaining return on investment (ROI) on their technology investments. AMI defines SBs as organizations employing 1-99 employees and MBs as organizations employing 100-999 employees.

Figure 2: Requirements of Technology Investments



Source: AMI-Partners, 2006

Notes:

PC-enabled Medium Businesses (PC MBs): N = 101 (Base = 1,271 PC-enabled MBs)

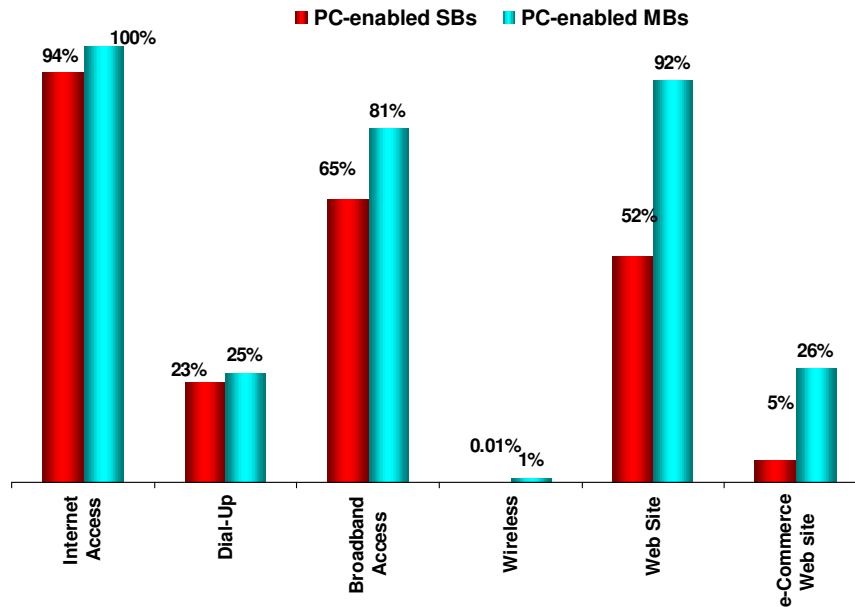
PC-enabled Small Businesses (PC SBs): N = 303 (Base = 0.10 Million PC-enabled SBs)

Chart illustrates only respondents who answered "very important" and "important".

On a positive note, we note that SMBs in Singapore have matured slightly in their decisions concerning IT. The importance of getting online and being connected on a regional and global basis has seen high internet penetration rates across SMBs.

Close to 95% of SBs have internet access and over 65% of these organizations are employing broadband access technologies. Internet access for MBs has reached saturation point, with 81% of these businesses using broadband access technologies (see Figure 3). With pricing for broadband access becoming increasingly competitive, and as users become familiar with employing this technology, it is expected that the penetration rate of broadband access will continue to rise at the expense of dial-up internet access.

Figure 3: Penetration by Access Type (SMBs)



Source: AMI-Partners, 2006

Notes:

N = 101 (Base = 1,271 PC-enabled Medium Businesses)

N = 303 (Base = 0.10 Million PC-enabled Small Businesses)

The importance of wireless has been noted by SMBs in Singapore. Indeed, 27% of MBs and 23% of SBs, when polled, said that implementing wireless LAN technologies and applications were important or very important to their company. This is because of the benefits this technology has over wired network access, including increased access, convenience, flexibility and lower cost.

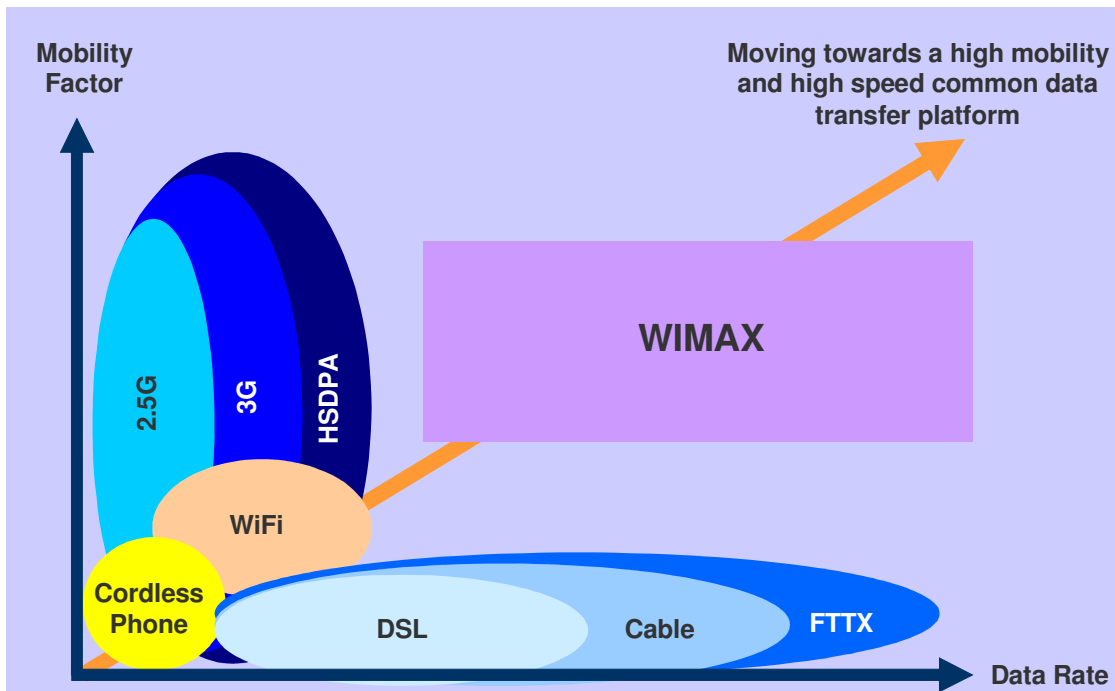
It is expected that SMB spending on wireless LAN will exceed US\$10 million by 2010, growing at a compound annual growth rate (CAGR) of 19% from 2005-2010. Key accelerators for wireless adoption include the following:

1. Wi-Fi chips being built into client devices (such as Intel Centrino into notebooks). Intel has recently announced moves to make WiMax cards for laptops available at the end of 2006.
2. Growing usage of VoIP and/or other specialized mobility applications.
3. Competitive pricing of wireless vis a vis wired solutions.

4. Familiarity with other wireless broadband technologies such as Bluetooth or 3G, spurring the growth of the wireless internet access market.
5. Initiatives by governmental bodies and industry players to promote and educate users about the benefits of wireless access. Recently, the Singapore government announced that high speed wireless surfing would be made freely available to all to encourage familiarity with wireless access.

It is thus a matter of time before broadband users migrate to wireless broadband. Figure 4 illustrates the evolution of Internet and mobile technologies. As technologies mature, users will be able to experience complete mobility and fast data transfer rates.

Figure 4: Evolution of Internet and Mobile Technologies



Source: Pacific Internet, 2006

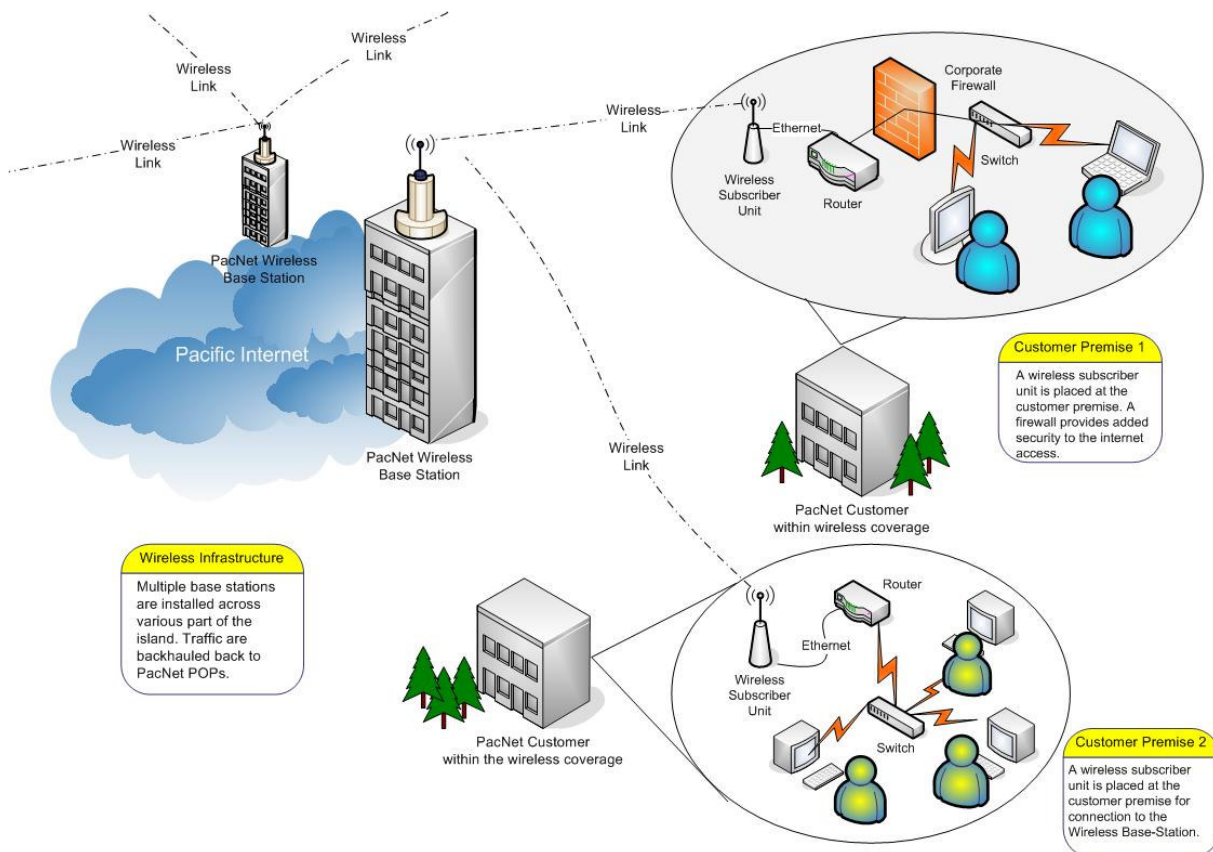
Wi-Fi and WiMax

To date, SMBs' experience with wireless has been through the use of Wi-Fi technologies, usually via wireless routers that are connected to a LAN. Wi-Fi (Wireless Fidelity) is a set of product compatibility standards for wireless LAN based on the IEEE 802.11 specifications and uses spectrum in the 2.4 GHz range to exchange data at broadband speeds. Users

access data through locations known as "hot spots". In Singapore, Wi-Fi networks use radio spectrum designated by the IDA for unlicensed operators. Short-range devices such as wireless LANs and modems are exempted from licensing, although they must be approved by the IDA.

WiMax (Worldwide Interoperability for Microwave Access) or IEEE 802.16 comprises several standards. According to the WiMax forum, IEEE 802.16a standardization focuses on fixed broadband access. IEEE 802.16-2004 enhanced the standard by providing support for indoor Consumer Premises Equipment (CPE). This flavor of WiMax primarily competes with cable modems and xDSL for residential and business access applications. The IEEE 802.16e standard, an extension to the approved IEEE 802.16-2004 standard, was approved recently in December 2005 and adds data mobility to the current standard. Figure 5 illustrates how users can access broadband wirelessly.

Figure 5: Fixed-Wireless Broadband in Action



Source: Pacific Internet, 2006

Being a carrier grade technology, WiMax offers a higher level of reliability and quality of service than are now available in typical Wi-Fi implementations. WiMax operates within a licensed spectrum and boasts robust security measures such as authentication, encryption, and key management systems. In contrast, Wi-Fi operates in unlicensed frequency and is more susceptible to security threats.

WiMax boasts the ability to facilitate faster data transfer than Wi-Fi, and, depending on bandwidth availability, may produce data transmissions of up to 70 Mbps, compared to 11 Mbps based on Wi-Fi (IEEE 802.11b standard) or 54 Mbps (based on IEEE 802.11a standard).

Currently, most service operators in Singapore such as Pacific Internet are offering fixed wireless broadband or "pre-WiMax" (see Figure 6). With the WiMax momentum picking up speed, and in conjunction with manufacturers such as Intel and AMD rolling out WiMax-ready chips, it is expected that users will be able to experience the benefits of fully mobile broadband in the next few years.

Figure 6: Evolution of Mobile Wireless Broadband Development



Source: Pacific Internet, 2006

Wherefore Wireless?

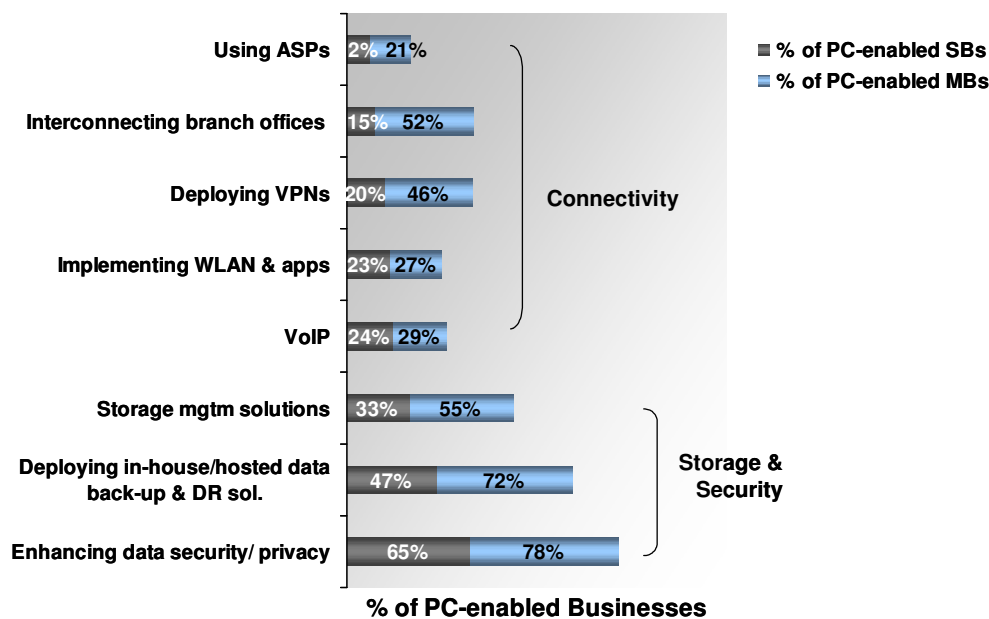
The benefits of wireless for SMBs cannot be ignored. Proponents of wireless broadband access note the following advantages associated with this technology:

- **High speed and wider coverage.** SMBs can access the Internet at speeds that dial-up access cannot match, anytime and eventually, from anywhere, without being restrained by “hot spot” locations. With wireless broadband technologies like those offered by services providers such as Pacific Internet, SMBs can access push/pull technology services, VPN, video-conferencing and VoIP applications. Both office workers and mobile field workers will be able to transmit and receive data quickly and effortlessly from any location without the constraints of wires.
- **Minimal support required.** Wireless access technologies are easy to install and deploy, with minimal resources needed to maintain it. Many solutions have been positioned to be “plug-and-play”, ensuring that even smaller SMBs are able to deploy this technology painlessly.
- **Affordability and ease of deployment.** Without the hassle of setting up networks, wireless access technologies are cheaper and faster to deploy, be it usage on a permanent or temporary basis. Businesses can use wireless broadband technologies as a backup or alternative to an existing leased line for the purposes of business continuity.
- **Increasing use of hosted software or storage solutions.** Over 20% of small businesses employing less than 100 workers, noted the growing importance of ASP usage. With wireless access technologies, businesses can increasingly access applications on a software-as-a-service basis.
- **Secured access.** Wireless broadband technologies such as WiMax operate within the confines of licensed spectrums and carrier-grade security, ensuring that data is transmitted securely to the users’ base stations. WiMax security supports certificate-based encryption standards including that of DES3 (Data Encryption Standard) and CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which essentially encapsulates data through encryption based on AES (Advanced Encryption Standard algorithm).

- Whether employing wired or wireless access technology, SMBs noted that security was a key consideration and certainly one that would impact all IT decisions (Figure 7). Security spending by SMBs is expected to grow at a compound annual growth rate of 17% from 2005-2010.

As far as penetration is concerned, security applications such as anti-spam and anti-virus have clearly gained traction within medium businesses with lower uptake in the smaller businesses. For the small business that often lacks access to a dedicated IT security expert, managing IT security issues can often be perceived as a daunting task, be it in a wired or wireless environment. In addition to perceived high costs of usage, lack of standards and interoperability, concerns about security represent primary inhibitors to the growth of wireless internet in Singapore.

Figure 7: Importance of Connectivity, Security and Storage



Source: AMI-Partners, 2006

Notes:

% of PC-enabled SMBs who answered "Very Important" and "Important".

PC-enabled Small Businesses (PC SBs): N = 302 / Base = 0.10 Million PC-enabled SBs

PC-enabled Medium Businesses (PC MBs): N = 101 / Base = 1,271 PC-enabled MBs

It is not surprising; therefore, that many SMBs have begun to explore managed security solutions. In such scenarios, the outsourced service provider takes responsibility for the security of the data network. With the appropriate service level agreement (SLA) in place, SMBs can safely devote their energies on their core business instead.

Preparing for the Wireless Wave

Whether it is Wi-Fi or WiMax, SMBs considering embarking on the wireless road should consider the following moves:

- Determine your organization's migration path from wired to wireless technologies and map the organization's needs to the technology available (Wi-Fi or WiMax) to ensure an optimal fit. Determine key performance indicators (KPIs) for your wireless investment such as lowering of infrastructure costs, increases in productivity and connectivity.
- Explore applications available (ASP/ VoIP) to ensure optimal usage of wireless technologies.
- Determine SLAs such as uptime performance and seek service providers that can provide such service level agreements.
- Partner with service providers that can provide a secure end- to-end wireless solution and ones that are reliable and trusted to ensure long term support and growth.
- Engage in trials and education of users before company-wide roll out of wireless technology.
- Ensure that security measures are installed with all wireless devices, especially at the user/client level. This will include the use of applications such as hardware and software firewalls, VPNs, intrusion detection solutions and desktop scanning software.
- Provide extensive education to users on how to keep devices secure as they are often the weakest link in network security.

About AMI-Partners

Established in 1996, AMI Partners is headquartered in New York City, with a network of offices and affiliates in Houston, San Jose, the U.K. (London), Japan (Tokyo), India (Kolkata) and Singapore.

AMI specializes in ICT solutions & Business Services, actionable market intelligence, and venture capital services focused on global SMB enterprises, extending into large enterprise. AMI's team of analysts and consultants boast strong functional experience in management and strategy consulting, business planning, market research, logistics, marketing and channel distribution, branding, venture investments, alliance partnerships and acquisitions.

Appendix 1: Security Problems

Common security problems associated with wireless networks include:

- **“War-driving”.** War-driving happens when users gain free Internet access or access an organization's data illegally, through driving around with a Wi-Fi equipped computer, such as a laptop or a PDA to sniff out or detect Wi-Fi wireless networks. In Singapore, war-driving may constitute offences under the Computer Misuse Act and the Telecommunications Act. A quick way of guarding against unauthorized access to your wireless network is to cloak your network. By default, wireless network equipment broadcasts a beacon signal that provides information necessary for devices to connect to it, including the SSID (service set identifier). Disabling the broadcasting of the SSID, or even the beacon signal itself, will make it harder for unauthorized devices to connect to your wireless network. Another method would include filtering MAC (Media Access Control) addresses. Because every device that connects to the internet has a MAC address, MAC filtering ensures that only devices with certain MAC address can access the Internet via your network. These measures act as deterrents but are not 100% effective against the determined hacker.
- **Client-to-client attacks.** Depending on how client devices such as laptops or PDAs are configured, wireless clients can communicate with each other, bypassing the base station or access point (AP). When configured to work in infrastructure mode, the client machine can only communicate with the AP that shares the same SSID as itself. In an ad hoc mode, a client machine will communicate in a peer-to-peer fashion with any other wireless device configured for the same SSID. In such instances, security can be compromised if any of the client devices are vulnerable. Short of physically checking on client devices on an hourly basis to ensure that client devices are in the more secured infrastructure mode or installing wireless sniffing devices to detect machines in ad hoc mode, administrators cannot prevent the end-user from configuring his/her machine otherwise. User education is the most important tool to manage such situations.