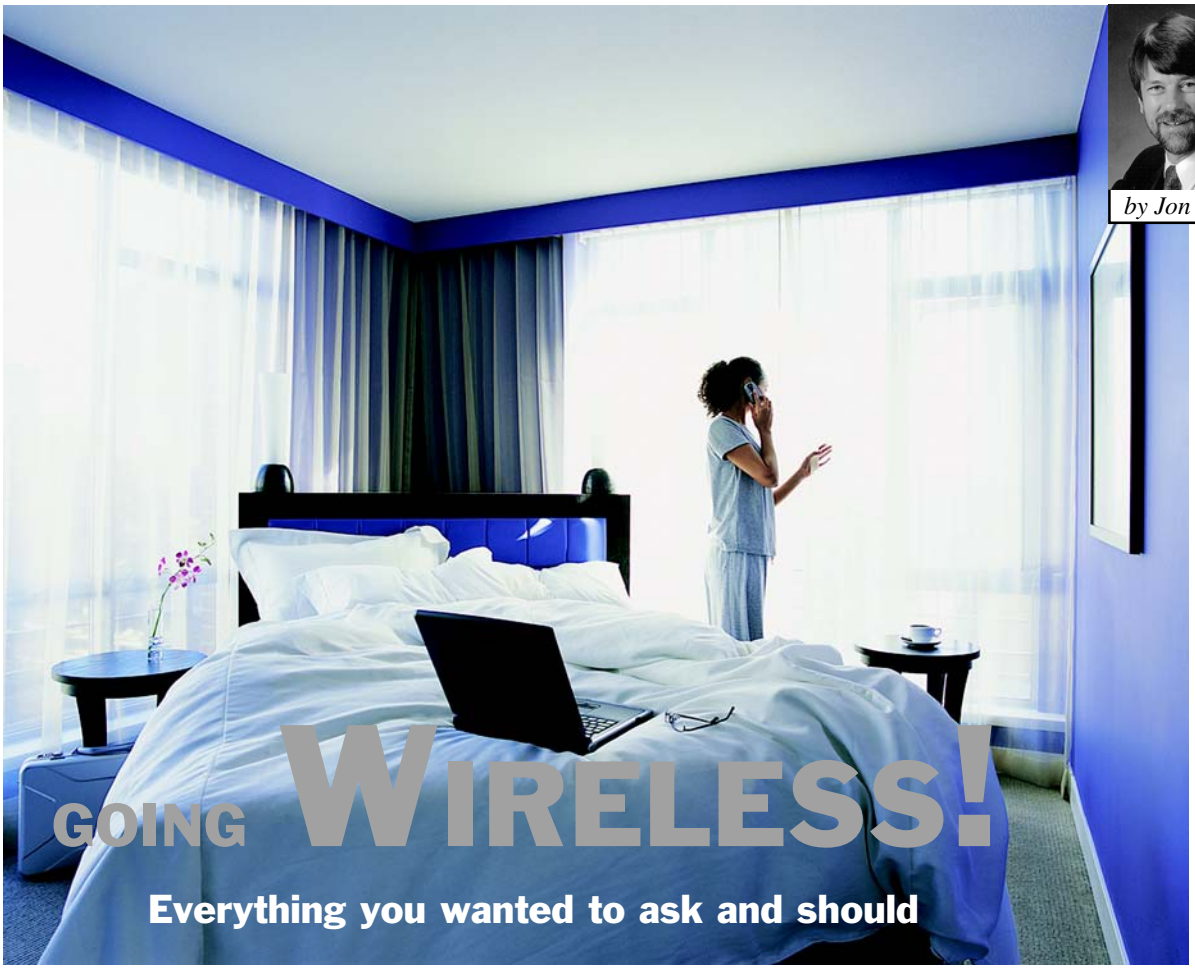


by Jon Inge

GOING WIRELESS!

Everything you wanted to ask and should

Wireless messages travel at the speed of light. Sometimes it seems that the technology itself changes just as quickly leading to all sorts of questions and confusion. What really matters in a hotel environment? Which systems do you need, whether for you or your guests, and what do you need to know to get the most value from these systems? Will they be obsolete three months after you install them? How secure are they? And what is a Bluetooth anyway?

Mention the word wireless to most people today and they will probably assume you're talking about linking laptop computers to the Internet or to a central server at their offices. While that is certainly a hot area, several wireless technologies play a significant role in the hospitality world. The ones you are most likely to find are: 1) high-speed wireless data networks for PCs, which are covered by a family of standards technically called 802.11 but more commonly known as WiFi (wireless fidelity); 2) cell phone links, which operate at much lower speeds and include both phones and data/e-mail communicators (such as RIM's Blackberry) that use the same networks; 3) Bluetooth, which is a low-power, short-range technology intended to link multiple peripheral devices over very short ranges (up to 30 feet), in effect replacing connection cables; and 4) Radio-frequency identification (RFID) where tags are used for inventory and purchasing control. RFID is still too expensive for practical hospitality use at the moment, but its eventual adoption is inevitable as costs decrease.

We will examine each of these wireless technologies, but start with the big one: wireless networks for computers.

High-speed Wireless Data Networks

The intensified level of interest in wireless connections over the last year caught many people by surprise. It seems that the availability of high-speed Internet access (HSIA), in some form or other, went almost overnight from a "nice to have" option for travelers to a definite selection criterion. Wireless connectivity is often the preferred choice over wired connectivity for the freedom of movement it offers, and hotels have been rushing to implement it at a speed that would have been unthinkable two years ago. There is also growing interest among hotel managers in exploring ways to use wireless networks to make their operations more flexible and efficient, both as a goal in and of itself and as a way of leveraging the investment in wireless networks for guest use.

Should You Install a WiFi Network?

The first thing to do when you're trying to decide whether or what type of Internet access to provide is to determine what your guests really want. What is your guest mix? Do your guests tend to travel with wireless-equipped laptops and congregate in outdoor areas, or are they predominantly staying in their rooms and only need wired access? What kind of networking and Internet access do your groups need in the function rooms, and with what level of security? Only when you have a firm

>>

grasp on demand should you look at your property's physical structure and start soliciting bids to implement the right mix of solutions.

Wired or Wireless for HSIA?

With the explosive growth of interest in wireless communications, it's almost a given that you will see benefits from installing wireless access in at least the public areas. People are beginning to expect such access in public facilities, and at the moment it can be a positive attraction to bring people to your property. As it becomes more widespread, not having it will become a negative. If people think you don't have wireless access they'll stay away since they will easily find it elsewhere. Don't forget that McDonald's has issued a request for bids to install wireless HSIA in every one of its over 30,000 restaurants.

Whether to install wired or wireless access in guestrooms is a question open to lively debate. If the owners of newer buildings had the foresight to install extra network cabling to guestrooms (or at least spare conduit and riser space) it can be relatively cheap to install a wired system. In many larger and/or older properties retrofitting cable to every guestroom for wired HSIA can be very disruptive and costly (although several HSIA vendors offer creative retrofit solutions that utilize existing wires, such as electrical, telephone or coaxial in guestrooms, to circumvent costly or impractical installation of new cables).

Older buildings with dense construction materials are more of a puzzle. While retrofitting cable is likely to be expensive, the structure could be dense enough to mask many wireless signals and require more than the usual number of access points for adequate coverage. Only a site-specific survey can tell you for sure. In any event, don't forget that even wireless networks still require cabling to be run to each access point.

What Standard Should You Use?

The 802.11 standard has been in use for several years, with different sub-sections covering different speeds and utility functions (see Wireless Glossary). Every new version is greeted eagerly since it usually promises faster connections, but the version with critical mass in the real world is still the original 802.11b, which gives a good balance of reasonable range (about 100 feet from a base station) and very usable speed (11 Mbps). Development of the newer, faster versions is worth keeping an eye on, but most businesses will be fine with 802.11b for now.

Given that this is still a fast-developing technology, though, how do you ensure against obsolescence? Stick with the major vendors who offer chip-level upgrades to later standards as needed. You're also more likely to have a reliable, well-functioning network if you stay with the big names, especially if you can go with a single vendor's

Continued on page 11

Several wireless technologies play a significant role in the hospitality world. They are:

- **high-speed wireless data networks for PCs**
- **cell phone links**
- **Bluetooth**
- **RFID**

Wireless GLOSSARY

Internet Protocol (IP) is the set of rules governing all communications over the Internet. Each computer wanting to use the Internet must have a unique IP address, a four-section number such as 192.168.112.205, to identify it. In open, unsecured public networks such as those in hotels and coffee shops, the communications server dynamically assigns a number to each computer as it requests access, which then keeps that number until it signs off from the session. On secured corporate networks the PCs (including laptops) are usually assigned fixed (often called static) IP addresses, often combined with specific encryption processes to form a virtual private network (VPN). The corporate servers then only accept access requests from PCs with the right IP address and right encryption.

802.11 is the IEEE (Institute of Electrical and Electronics Engineers) standard for wireless data communications. The most relevant sections are:

802.11b – the most widespread standard, for transmissions at speeds of up to 11 Mbps and using the 2.4 GHz frequency band

802.11a – much faster, with speeds up to 54 Mbps but using the 5 GHz band, with much shorter range than 802.11b and not compatible with it

802.11g – a more recent development of 802.11b offering speeds up to 54 Mbps, using the same 2.4 GHz band as 802.11b and compatible with it but with somewhat shorter range

802.11n – a proposed new standard for speeds from 100 Mbps to 320 Mbps, expected to be released in 2005-2006

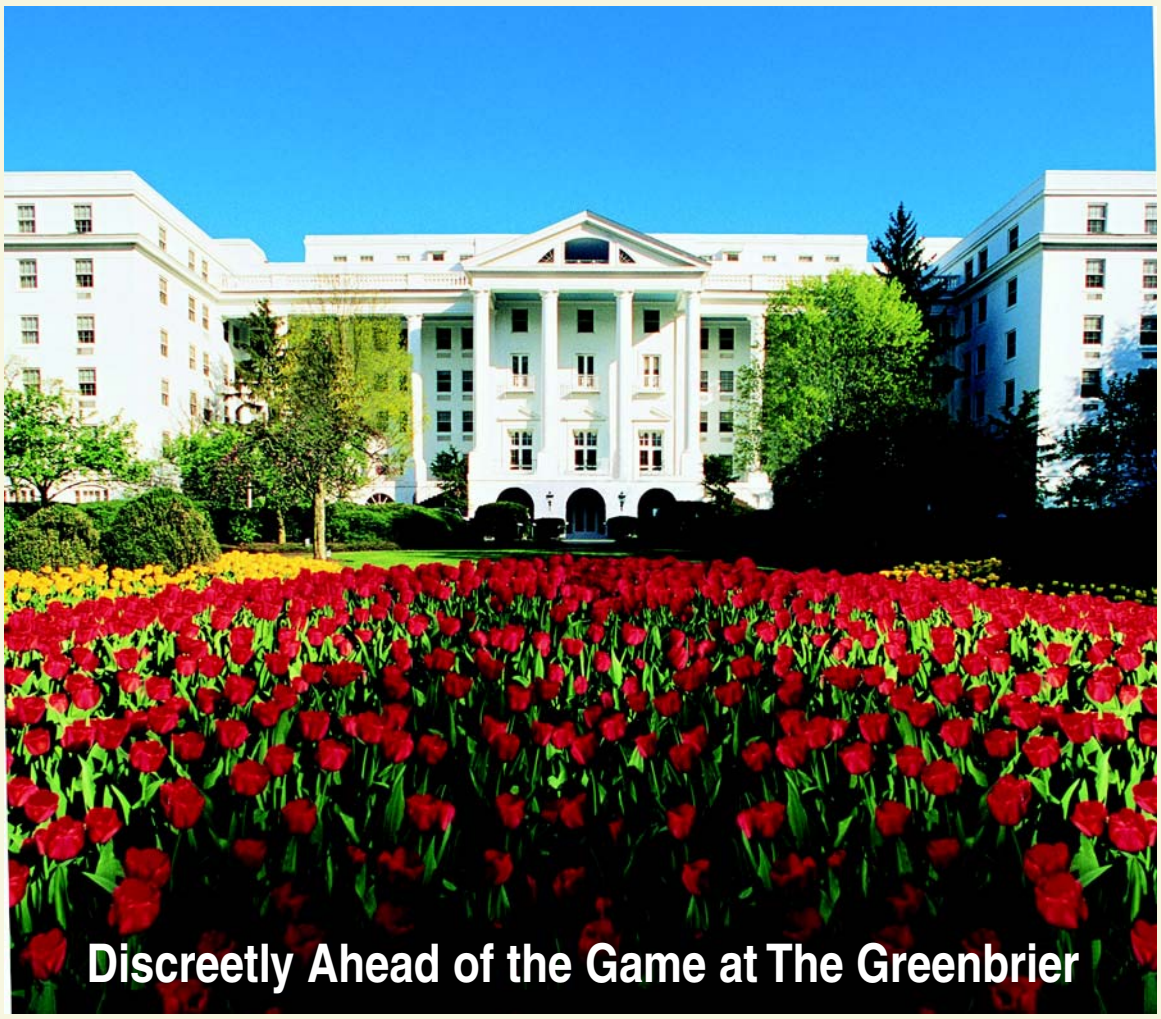
802.11i – a proposed standard for improved wireless security, expected to be ready mid-2004

802.11e – a proposed standard for various quality of service levels

A new wide area wireless network standard, 802.16, was approved in January 2003 and is being promoted as **WiMax**, somewhat dubiously labeled as an acronym for worldwide interoperability for microwave access. WiMax networks are planned to have a range of up to 30 miles with data transfer speeds of up to 70 Mbps, but preliminary testing isn't expected until late 2005.

WEP vs. WPA These are the two current standards for wireless security. WEP (wired equivalent privacy) was the first widespread wireless encryption standard. While a useful mechanism to keep out random searchers, it can be broken relatively easily by someone with the right tools. The more secure WPA (wireless protected access), now available from most network equipment vendors, is an early-release sub-set of the pending 802.11i standard.

Service set identifier (SSID) is a fancy term for the name you give to your network, which appears on users' computer screens when their wireless cards detect the presence of the network. Since it's common for cards to pick up several wireless networks at once from a single location, it's important for your hotel's SSID to be clear and obvious.



Discreetly Ahead of the Game at The Greenbrier

You would be hard pressed to find a more traditional operation than the fabled Greenbrier in White Sulphur Springs, West Virginia. Home away from home for Presidents, captains of industry and the elite for centuries, the stately resort exudes Old World charm and service. So it comes as something of a surprise to find that it has offered property-wide wireless high-speed Internet access for well over a year.

"We wanted to offer HSIA to the small but growing number of guests requesting it," said Mike Keatley, manager of information technology. "And the hotel's structure made it much easier to implement that through a wireless network. We launched the service in October 2002 for the main hotel guestrooms, quickly added the conference rooms and are now extending it to the guest cottages."

How many guests take advantage of the service? "Last year we recorded 4,300 guest days of usage," said Keatley, "and it's growing really well. Initially it was unusual for guests to have wireless cards in their PCs, so we've always kept a stock of cards to loan them. We also had someone available onsite to help with any configuration issues, which are usually pretty minor. Now we're seeing that around 40 percent of guests requesting access have their own cards. That percentage is also increasing rapidly."

Keatley talked about the other wireless technologies The Greenbrier is using. "We're planning to piggy-back some adminstration functions, such as housekeeping and engineering communications, over the same wireless network with suitable security and isolation from guest usage, of course," said Keatley. "We're already using a point-to-point wireless link to provide a POS workstation at the golf course halfway house with a real-time connection to the main system, and we have experimented with wireless check-in terminals."

"We're also working hard to improve outside communications to the resort," Keatley said. "Located in a somewhat remote valley, cell phone coverage is not as good as we'd like, but we recently put up a communications tower for a new circuit and can now offer Blackberry service throughout the property."

The Greenbrier strives to be as close to the leading edge of technology as it can, without being obvious to the guests except in the levels of service it provides. "Wireless technology really helps us fulfill that goal."

products for the complete system. Interoperability between different vendors' product lines is supposed to be a given, but it's still more of a promise than fact.

What's Wireless Used for?

Usage by guests is pretty straightforward. Most individuals simply access the Internet or retrieve their e-mail, while groups often use it to set up ad hoc local area networks (LANs) in a meeting room to share documents.

As for management systems, since WiFi is merely an extension of an existing wired network, any application has the potential to use wireless terminals if there's some operational benefit to justify their additional cost. Some examples are:

Property Management Systems: Wireless check-in/check-out workstations were extensively tested a year or so ago, but while they worked well most trials have been dropped. In many cases it proved more cost effective to install spare wired network points in locations where a workstation or laptop could be quickly plugged in to handle front desk overload situations. In some circumstances wireless units have real benefits. For example, at a spread-out property shuttle buses can pick guests up from an airport or railway station and check them in as they're being taken to their rooms, avoiding the stop at the front desk.

Point of Sale: Handheld units for restaurants and bars have been in use for at least 15 years and save considerable time placing orders in spread-out operations. Older models used slower protocols running at 27 MHz or 460 MHz, which had good range but tied each handheld unit to a single access point. More modern units have migrated to WiFi, especially as the vendors started using generic Palm or Pocket PC units instead of building their own devices. While these have shorter range, requiring more access points for the same area of coverage, they allow more operational flexibility since they can roam from one access point to another without losing contact.

Housekeeping and Engineering: There are considerable benefits for equipping housekeeping and engineering staff with wireless handheld units. Housekeepers can be notified instantly of changes in room cleaning priorities and can notify engineering at once of maintenance tasks they notice during room cleaning. Minibar re-stockers can post usage charges to the PMS directly from the room, or be advised of any specific stocking requests for an arriving guest. Engineering staff can be advised immediately of new work orders and can have access to any item's maintenance history or technical manuals online.

All of these benefits don't come free. While they are technically straightforward, the costs of the handheld units and of ensuring wireless network coverage throughout the building, especially in the lower basement floors where these departments are usually based, can be significant. Each property has to evaluate its own situation weighing implementation costs against its particular efficiency improvements.

Designing an effective handheld unit is a particular challenge. Tablet-sized PCs show the full screens of the underlying software application and are simple to install. While they require no training they are bulky and heavy. Smaller PDA-based devices are more convenient, but then screen design becomes the critical issue because only a sub-set of the main application is shown at a time.

Ruggedized units like the ones manufactured by Symbol Technologies are durable and effective, but are also bulky and not particularly attractive, which can be an issue if they are intended for guest service in upmarket hotels.

Pocket PCs or Palm units are far more visually appealing and versatile, but are expensive, break when dropped and are liable to disappear because they are identical to consumer PDAs. Issuing them only to managers or senior staff can be a good compromise in a large property where efficiency benefits can be fully realized.

Implementing an Effective Network

Since wireless networks are still just extensions of wired ones, a high-speed link to the Internet starts with a wired connection. This connection is usually a telephone T1 or DSL (rated at 1.5 Mbps and up to 1 Mbps, respectively). These are usually supplied through a contract with your telecom vendor.

Note that the speed of the incoming connection is another reason not to worry too much about going with the faster versions of WiFi. However much you improve the wireless link between the PC and the access point, the link to the Internet looks like a bottleneck. In practice a single T1 line can provide perfectly satisfactory access for several dozen simultaneous users. You need to monitor peak and average traffic to make sure you are providing an effective service. Your telecom vendor should provide regular reports on this data.

It's best to set up physically separate wireless networks for guest and administrative usage. This costs more than relying on the network software to separate the two, but it ensures that no one on the guest network can hack through to the administrative side and review or corrupt sensitive files.

You will need a gateway/server to control wireless and Internet traffic. Using the gateway you can display a hotel-customized welcome screen for users offering links to hotel-related services as well as providing access to the Internet. If you want to charge for access the server will need a PMS interface. Each guest's or group's access must be kept separate from other users on the same network, but this is straightforward with modern servers, which treat each connection as an independent virtual LAN (VLAN).

The most critical items, though, are the access points (APs), the small base stations placed around your property to act as transmitters/receivers to link mobile computers to the wired network. If you keep in mind that the most widespread version of WiFi

>>

Pocket PCs or Palm units are far more visually appealing and versatile, but are expensive, break when dropped and are liable to disappear because they are identical to consumer PDAs.

(802.11b) has an effective range of only about 100 feet, it becomes obvious that for effective coverage over any significant area you'll need quite a few APs.

Placing these access points requires expertise. It can be tricky to predict how signals will be affected by a building's structure, and dead spots can occur unexpectedly forcing the installation of additional APs to fill in the gaps. It can also be a challenge to run network cable to the best location for an AP, perhaps requiring some extra units in less-optimal positions (or even a wireless bridge) to ensure coverage of the problem area. A detailed site survey is critical to ensure good, reliable service.

Don't stop with a pre-installation survey. Coverage must be checked post-implementation and at routine intervals thereafter to make certain that the areas you tell your guests are covered actually do provide service. One unexpected bonus of intermittent surveys is that they will identify any rogue wireless networks your staff may set up on their own for personal HSIA access outside your policies and restrictions.

The access points' transmission strength also should be adjusted so that one doesn't overpower another, and so you don't provide access any further outside your property than you intend. For rural properties this isn't usually a problem, but in a city center site you don't want to offer free Internet access to workers in the adjacent office building. While it's good to advertise that you're providing this service for your guests, having too many non-guest users on the network can slow it down, especially if they start downloading videos.

Assigning a clear identification name for your network is essential when configuring it. Either the hotel name or the service provider will suffice, as long as the latter is made clear to the guests on tent cards or through some other notification as to who is providing the service. Calling the network "base" or "HotelName1" when you have a number of other "HotelName" networks active for administrative use doesn't help anyone pick out which network they're supposed to connect to.

User-related Connectivity Issues

Hotels should keep a few spare wireless cards available (either free or for rent) for guests who don't have built-in connectivity in their laptops, as well as basic configuration instructions. Each vendor offers a toll-free number for assistance with guest set-up and configuration, but it's a far better guest service if someone at the hotel can also help the guest directly.

With connectivity problems keep in mind that the guest's laptop may have wireless technology built-in and it just hasn't been configured properly. The fact that many corporate laptops are set up so that their users can't change the configuration complicates matters further.

How About Security

Enforcing encryption on public access networks is impractical. It may interfere with other encryption required for corporate users to access their companies' networks over VPNs (virtual private networks), which provide secure communications from laptop to corporate office. Just as with airport or coffee shop networks, therefore, hotel guest wireless networks are not secure, leaving the users open to having their systems hacked and private information stolen by determined individuals.

This shouldn't come as a surprise to any user, but for liability purposes it's important to ensure that guests are informed, usually on the initial sign-on screen for the service, that the network is not secured and that they transmit any personal information over the network at their own risk. Travelers who worry about security must take responsibility for it themselves.

Important precautions for any traveler include using a personal firewall (such as those from ZoneAlarm or Norton) on their laptop, disabling the Windows' file sharing option, keeping anti-virus software and security patches up to date and staying acutely aware of what they're sending. But it's not the hotel's responsibility to make sure their guests' PCs are suitably equipped and configured.

However, taking the everyday viewpoint in a parallel with cell phone usage, it seems that few people care about these security issues. The huge convenience of being able to communicate anywhere they happen to be outweighs any caution they might have over the security of their conversations, spoken or electronic.

>>

Wireless Support

It's important to make sure that your support arrangements cover:

__ Remote network monitoring

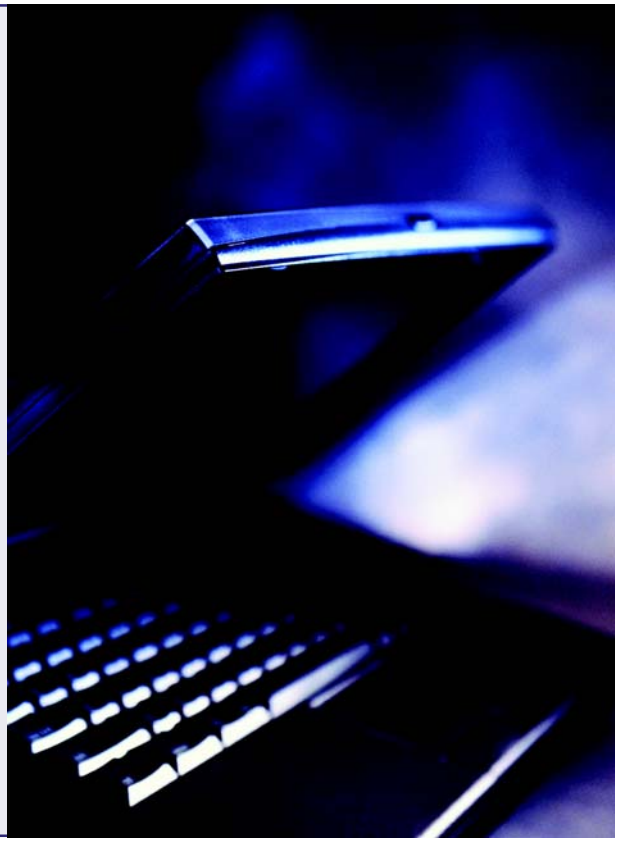
__ Network support, including switches and interfaces

__ 24-hour user support (usually charged on a per room basis)

__ Server/gateway support (often includes software upgrades)

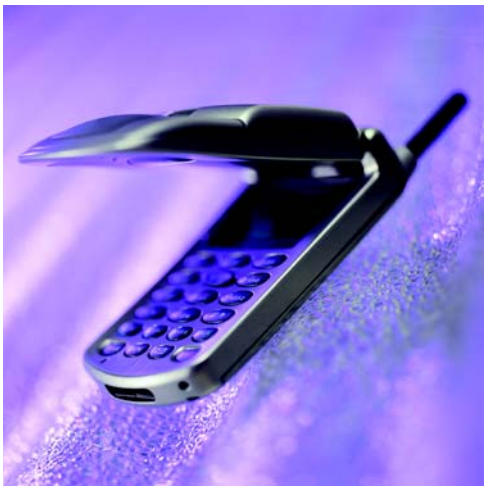
__ T1, DSL or cable HSIA circuit maintenance

Some of these components may be maintainable by in-house staff, others may fall under more than one vendor agreement. Most wireless HSIA vendors monitor your network constantly from a central site, down to the individual access points throughout the property. This allows them to report on traffic patterns so you can identify any anomalies or problem areas. The outside connection is usually monitored by the telecom vendor separately from the HSIA vendor.



To Charge or Not to Charge

The initial approach many properties took was to charge everyone around $10 for 24-hour access. But on-going debate has escalated over whether revenue is maximized through collecting add-on charges or through providing free access to attract guests and boost occupancy. It's something of a paradox that most hotels currently charging for access are the full-service brands and high-end resorts. Their guests can more readily afford it, but they are may also be more likely to resent being nickel-and-dimed for add-on charges. The lower-end properties, that presumably could use all the revenue they can get, generally give Internet access away. A great deal in determining the most advantageous policy depends on each property's guest mix and the level of demand that goes with it.



Another consideration is whether to offer guests service from a virtual network such as iPass or Boingo. These vendors don't have networks of their own but form coalitions of different network providers that offer their users wider geographical coverage than they'd get from one vendor, for a single monthly charge. Several corporations have accounts with these companies and require their travelers to stay at hotels that are participating members. Many HSIA vendors offer the option and it can certainly bring additional room nights to your property, but if you normally charge your guests for HSIA you won't be able to do so for iPass or Boingo clients.

Other Wireless Communications

Cell Phones

Cell phones operate at much lower data transmission speeds, from 40 Kbps to 400 Kbps depending on the service provider and type of phone, and at frequencies of 800/900 MHz and 1,900 MHz. Cell transmissions cover a much wider area than WiFi, which means that you can often pick up a cell phone signal even if you can't send much data over it very quickly.

While cell phones aren't compatible with WiFi links, they can act as modems to connect laptops to the Internet. It's not as fast (running at much the same speed as a conventional dial-up modem) but it can provide a useful connection where WiFi isn't available.

There has been a tremendous convergence of mobile technologies and devices as cell phones and PDAs merge. Several Blackberry models now have voice functionality, and many cell phones have PDA-like data collection and management capabilities. Adding to the confusion, various PalmOne and Pocket PC PDAs now have connectivity options, but in three different forms: some have cell phone functionality to take on the Blackberries and data-ready phones; some are available with built-in WiFi communications for use as personal workstations on a wireless data network; and others have Bluetooth capability (see the next section) and can link wirelessly to a cell phone for dial-up access or to a WiFi-equipped laptop for high-speed network connections. It's fascinating to speculate where this will end up, but the emergence of some form of universal handheld communicator seems inevitable.

Bluetooth

Named for a Danish king who united Denmark and Norway circa 975 A.D., this technology is intended to link multiple peripheral devices over very short ranges (up to 30 feet), in effect replacing connection cables. Wildly over-hyped on its initial introduction, Bluetooth has now matured into a reliable and convenient way to link cell phones to headsets or laptops, to provide sophisticated remote control of data projectors or to synchronize data between cell phones, laptops and PDAs.

It operates in the same 2.4 GHz frequency band as the mainstream 802.11b WiFi technology and many cordless phones, but with a different, incompatible transmission protocol and a much slower data transfer speed of up to 720 Kbps. Early implementations had some interference problems and could slow down WiFi transmissions significantly, especially in areas where the WiFi signal is weak. But these issues have now been resolved through cooperative developments between vendors.

Bluetooth devices automatically recognize each other, but must be granted permission to communicate. Since it is essentially a personal convenience link, hotels don't need to do anything to accommodate their guests' use of it, except perhaps to ensure that data projectors they rent for meetings are Bluetooth capable.

Radio-frequency Identification (RFID)

On the horizon is the use of RFID tags for inventory and purchasing control. These tags contain more information than a bar code label. Information carried with RFID can be detailed information on the goods they're attached to or the conditions the items have encountered in transit, such as excessive temperatures or shock loads. The prime advantage of RFID is their ease and speed of reading. Usually not powered themselves, they generate enough internal energy from an interrogating radio signal to transmit their data, thus allowing a wireless gateway to identify every item on a pallet of goods passed through it without having to check each item individually or even to have the labels visible.

The technology promises very significant improvements in purchasing efficiency, but at this stage it is still too expensive for adoption by most organizations. The identification tags themselves cost at least 25 cents, and wireless gateways to interrogate and track them can run up to $200,000 each for a major warehouse. Use will become widespread as costs come down, driven by major investments from the early adopters. For example, Wal-Mart, the U.S. Department of Defense and German supermarket chain Metro AG have all mandated that their top suppliers must deliver goods only on RFID-tagged pallets by the beginning of 2005. Several smaller suppliers have asked to

>>

IMPLEMENTATION Issues

Wireless installations are usually less labor-intensive than wired ones, but there are still many potential pitfalls. Here are a few key factors to keep in mind:

Dead spots:

Problem: Wireless dead spots show up after installation.
Recommendation: Prevention is cheaper than correction; thorough site surveys before installation are essential. If the property is under construction, studying the plans should help anticipate possible trouble areas, but it's a good idea to repeat surveys at various stages of the construction to limit potential problems before walls are enclosed and additional cable runs become expensive.

Foliage and water affect wireless coverage:

Problem: Most people know that concrete and steel can block transmissions, leading to gaps in coverage; few are aware that foliage can be just as much of an inhibitor.
Recommendation: Make sure your wireless coverage testing includes areas where large bodies of water and foliage will be present and think about foliage growth. Small shrubs and trees have a habit of getting taller.

Cable properly:

Problem: It's not always easy to run cable to all the access point locations needed for the desired wireless coverage. Makeshift solutions, substandard cabling and running cables beyond the specified maximum lengths all cause problems.
Recommendation: Once again, a quality site survey can identify potential problem areas, and lets you work with the wireless provider ahead of time to define solutions (such as wireless bridges) that avoid potentially expensive construction modifications. Use qualified cabling contractors who accurately document their work.

Inadequate post-installation testing:

Problem: Many vendors don't conduct adequate testing after installation, leaving guests and users to discover dead spots and connection issues on their own.
Recommendation: Insist that the installer check all contracted areas of coverage to ensure that the signal is strong and that users will be able to connect. The installers should document the areas tested and report on signal strengths and data transfer rates.

Outdoor installations:

Problem: While outdoor wireless antennae are designed to withstand harsh environments, many of the network access points they're connected to aren't.
Recommendation: Make sure you have adequately protected locations to place the access points and mount them in weatherproof plastic boxes.

Budget for quality:

Problem: Focusing on the lowest cost solution usually results in an inferior product, through skimping on site surveys and installing non-commercial equipment. This can result in signal strengths that fade in and out, lower data transfer rates and limited area coverage.
Recommendation: Don't skimp. Add in proper site surveys and post-installation testing even if they're not in the vendor's bid. In most cases you get what you pay for. You may get lucky, but that's a bad gamble when providing such a high-demand guest service.

Help in preparing these tips was provided by Jeremy Rock, president of the RockIT Group, systems implementation consultants. He can be reached at (310) 575-0550 or jrock@rockitgroup.com.

be included in the program so that they too can take advantage of its efficiencies. The use of this emerging technology can only spread.

Where Do We Go from Here?

It's often said that wireless technologies are hyped, but there is no argument that they are making significant and fundamental changes in the way we live. There are huge conveniences to unhindered mobile communications that allow us to always be in touch with whatever information we need.

But we need to exercise caution as well. Being constantly in touch means that the networks continuously know where we are and what information we are requesting. We need to be vigilant about the potential misuse of this highly useful technology, or tools become our masters and their multiple benefits become tainted by our loss of privacy.

Jon Inge is an independent consultant specializing in property-level technology. He can be reached by e-mail at jon@joninge.com or by phone at (206) 546-0966.