

# Guest Internet Access

Getting There  
Bringing Internet Access



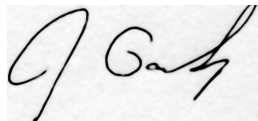
**Technical Issues,  
Costs, Terms and  
Definitions for  
Providing Guest  
Internet Access**

James Ganley  
Copyright 2008  
CheckBox Systems  
[www.4EZWiFi.com](http://www.4EZWiFi.com)

Providing Internet Access for your guests is a recent phenomenon for the hospitality industry. A little more than ten years ago the Internet was the realm of governments, universities, and a few hobbyists. Today it is a necessity for businesses and their employees, students, travelers, and therefore, you, if you want these people as your guests.

Providing Internet Access DOES NOT have to be difficult or expensive. It is not rocket science, despite what many networking professionals would lead you to believe. It does take a little bit of forethought and planning, and like any aspect of your property there will be occasional maintenance. Properly done, providing Internet Access for your guests will be one of the less expensive amenities you can provide, and can generate higher levels of guest satisfaction.

This booklet is designed to acquaint you with some of the basic terms and technical issues with providing Internet access for your guests. It is a good primer to help you plan to add Internet access for the first time, or if you are replacing a system you already have.

A handwritten signature in black ink, appearing to read "J Ganley", is positioned above the printed name.

Jim Ganley  
CheckBox Systems  
[www.4EZWiFi.com](http://www.4EZWiFi.com)

## **Different Ways of Providing Internet Access for your Guests**

There are several ways to provide internet access to your guests.

**Providing a phone jack for dial-up internet** - Providing a phone hookup for guests to use is one of the original ways to provide internet access. This provides the slowest form of internet access, and not all guests will have a subscription to a dial-up internet service provider. Guests plug their laptop into the phone jack and dial into their Internet Service Provider. For this to work, the property owner must supply a dedicated analog phone line. If the phone line is in the guest's room, then the guest can be billed for the cost of the call, if any. If the phone line is in a common area, then the phone line should have toll restriction, to prevent guests from running up long distance charges if their ISP is not a local call. Only one guest can be on line per phone line, and several guest on-line at once can end up tying up all of the properties' phone lines.

**Providing computers for guests to use** - Some properties will provide computers in a common area or a business center connected to the internet for guests to use. The internet connection can be dial up or high-speed broadband. These computers may also be networked to a shared printer so guests can print out documents. These computers must be locked down so that guests can not install software or other applications which could damage the machines. These computers must also have strong anti-virus software, and will periodically need to be wiped and reloaded with their software. These computers should be in an area that is within view of the front desk, physically locked down, and a written acceptable use policy should be posted.

**Providing wired high speed connections for guests to use** - Providing a wired, high speed connection to your guests allows you to share one incoming high speed connection among your guests as well as your office. These wired connections may be located in a common area, meeting rooms or distributed throughout the property. Installing wired connections in new construction is less expensive than retro-fitting existing properties. Wired high speed connections can sometimes be "piggy-backed" on top of existing cable or telephone lines running throughout the property, saving the costs of running additional cabling.

**Providing wireless high speed connections for guests to use** - Most laptops are now equipped with 802.11 wireless radio cards, that allow them to connect wirelessly to compatible access points. The quality and range of these wireless cards vary, and can be as little as 25 feet inside a concrete building, to over 1,000 feet outside in a field. Wireless networking is the most cost effective way to provide high speed access, particularly in existing properties. Wireless connections can be affected by radio interference.

It is not unusual for a property to provide more than one means for a guest to connect; Some may provide a wireless connection through the property, and have high speed wired jacks in meeting rooms and a business center in the lobby. Others may have a phone jack in the clubhouse for users still on dial-up, as well as high speed wireless in all of the common areas. Most newer properties are going all wireless, and providing wireless connectivity throughout the property for their guests to use.

## **Show Me The Money**

Making money from something you can't charge for.

The early days of high-speed internet in public areas spawned a "Gold Rush" mentality. Many companies thought they could get rich charging for internet access for people on-the-go. And like most of the early gold diggers, many of these companies have gone bust.

In certain premium locations, such as airports, where there is a captive audience with corporate expense accounts, you can still charge a premium for internet access. But for other users they are either unwilling to pay \$9.95 or so per hour, or they can simply wait until they get somewhere else. However the pay-for-play model can still work in some locations if the cost of access is reasonable.

**The Candy Bar Theory** - One smart property owner came up with what he called "the Candy Bar Theory". Most people don't think twice about spending a dollar on a candy bar or a bottle of water. If you make internet access cheap enough, like a candy bar, guests won't think twice about buying it. This successful operator charges \$1.95 for one hour, \$2.95 for one day, and \$6.95 for one week. Nobody ever buys just one hour, because for one dollar more they can get a whole day. And most of the guests that are there for more than two days just pay for a whole week.

**Setting Them Free** - Many properties are moving toward "Free Internet Access". Of course it is not really free, it is built into the daily or weekly rate the guest is charged. But because they are not being charged separately for it, most guests feel better about the "Free Internet Access", and will choose a location with "Free" access over a location that charges separately for access. One thing about free - more people will use it. So properties providing free access will have to plan on higher usage rates.

**Free, But Not Unlimited** - Some properties are successfully using a mixed model, where some access is provided free, and additional access is charged for. For example, each guest may be given 30 minutes of free access per day, and then charged for extra time. This allows most guest more than enough time to check email, and go to their favorite web sites, and allows you to charge the heavy duty users a premium. This also helps prevent some of the higher usage (and potential abuses) that can come with an all-free-all-you can-eat model.

**Customer Expectations** - When we pay for something we expect to get it. Occasionally there will be problems that prevent customers from getting online, problems ranging from equipment and ISP issues, to problems with the customers own laptop. Customers paying for access will be more demanding, whereas customers getting access for free may be less demanding. In the long run building the cost of internet access into the daily or weekly guest rate may be simpler than trying to charge guests a la carte for access.

## The Costs of Providing Internet Access

There are several costs involved in providing Internet Access for your guests. These costs will vary depending upon the size of the property, the volume of usage, and the vendors used. It is best to know these costs up front before purchasing a system. Over the lifespan of a system recurring and maintenance costs can easily exceed the initial purchase cost. If you are a seasonal operation you will want to determine if any of these recurring costs can be suspended in your off season.

**Purchase and Installation Costs** - Purchasing and installing your system includes not only the equipment and labor to install it, but also other costs, such as running electrical service to access points, installing poles or other structural changes as required by the vendor, and lost revenue if you have to take rooms out of service while cabling is done. Make sure you understand what your vendor will provide for installation and what else is needed. Often system installers can not do electrical work, such as running new power outlets, and many will not do structural work, such as installing poles. Make absolutely sure your installers are bonded and licensed for your location.

**Recurring monthly or annual costs** - Some vendors require a monthly or annual service fee or contract when you purchase their system. Here it is important to understand that some hotspot systems are **Hosted**, and some are **Self-Contained**.

Hosted systems rely on databases, technology and servers located at the vendors headquarters, and will require ongoing hosting and maintenance from that vendor for the life of the system. Even though you may own the hardware on your property, without the hosting and support of the vendor your system will cease to function. You will be paying recurring fees to the vendor, and these fees may or may not also include guest support and the cost of bringing in the Internet service to your property.

Self-contained systems contain all of the intelligence and technology in the hardware you own on your property, and do not rely on technology hosted by the system vendor. The system vendor may or may not require monthly or annual support fees.

**Maintenance Costs** - Your hotspot system will require some form of maintenance to keep it running smoothly. Typically maintenance consists of software updates and periodic checks of equipment and signal levels. Software updates will have to be provided by the system vendor and the cost may or may not be included in the monthly or annual maintenance costs. Signal and equipment checks may be done by the vendor, but can usually be easily done by the property owner.

**ISP Service** - The ISP is the company that actually brings the internet connection onto the property. Few hotspot vendors are also ISPs. In most cases a local ISP will be used to bring the internet connection onto the property. Usually the ISP cost will be the responsibility of the property owner. In some cases it may be built in to the recurring fees charged by the vendor.

**Guest Support** - If guest support is not built into a recurring monthly charge, the vendor may charge for it separately or offer it as an optional service. If you are providing free internet access you may find you do not need to provide guest support.

## Exercising Control

There are several different aspects of Internet access for your guests that you need to exercise control over; Who is allowed online, for how long, and how much bandwidth they are able to consume. Any guest Internet access system must be able to control these factors.

Uncontrolled access to your system can lead to guests downloading excessive amounts of data, slowing down access for other guest. It can also lead to guests abusing your internet connection to send millions of spam emails, either intentionally, or unknowingly, if their computer is infected with a spam generating virus.

If you are providing wireless Internet access it is important to remember that the wireless signal does not necessarily stop at your property line. Without some form of control, users other than your guests may be able to log on and use your Internet connection.

Controlling who is allowed online allows you to prevent users at neighboring properties or individuals just driving by or parked in the street from using your system. If you are charging for access it can also prevent your guests from using the Internet access for free. Most access control systems will include a captive portal. A captive portal captures the users web browser and redirects them to a designated web page, no matter where they try to surf to. All the user does is open their web browser and there are brought to the welcome page.

This designated web page is typically set up as a welcome screen, and invites the user to either get an access ticket at the front desk, enter their credit card information, or take some other action to authenticate them on the system. Some system vendors control and brand the page with their logo and graphics, others allow the property to design the page and customize it for their needs.

Controlling how long a guest is online allows a property owner to ensure that when a guest is no longer a customer they are no longer able to use the properties' Internet connection. It also allows a property to sell different increments of access time at different prices, to give away access for a limited period, and charge for additional access (i.e. "free 30 minutes of Internet access with each meal purchased, or 1 hour of free Internet access every day").

Controlling how much bandwidth a guest uses is very important to provide fair and solid access to all of your guests. Most users will use very little bandwidth, checking their email, browsing web pages or online chatting. A small minority of users will consume very large amounts of bandwidth, trying to download large movie and music files, watching streaming video online or intentionally or unknowingly sending millions of spam emails, if their computer is infected with a spam generating virus. Bandwidth control must be used to ensure that no one user is monopolizing all of the bandwidth on the system and slowing down other users, and also to ensure that no one user is using excessive bandwidth for abusive purposes.

If you are using a metered Internet service (such as some satellite providers), one that only provides a set amount of bandwidth per day to your location, then it is very important not to allow your guests to consume too much bandwidth. One guest downloading a large file could consume the entire allocation of bandwidth for the property for the whole day and shut down Internet access to the entire property for the rest of the day if bandwidth controls are not in place.

## Signal Strength, Power Levels and Antennas

Data communication between your guest's laptops and a hotspot is a two-way affair. For a successful connection not only does a signal need to get from the hotspot to the user's laptop, but they need to get a signal back to the hotspot. Laptop wireless cards are not all created equal and few have an external antenna. Therefore it is not unusual for a guest to "see" a signal of a few bars, or "good" on their laptops but have a difficult time maintaining a connection. This is usually a case of the laptop seeing the signal from the Hotspot but the Hotspot not being able to see the Laptop.

Another issue wireless users often encounter is the "signal strength" meters displayed on their screens. These signal strength displays are an approximation of the signal strength averaged over a period of time and do not take into account signal noise, the interference inherent in every radio transmission. This can lead to users seeing a strong signal displayed, but still not being able to establish a connection.

Of course just the opposite can occur; sometimes users will see a weak signal but yet make a solid connection. Regardless of what the signal strength display reads the bottom line for the user is always this: Can they connect and is the connection fast enough?

One way to improve the range of the signal is by adding a long range antenna to your access point (the access point in this case is the hotspot system). Long range antennas are rated in "dbi" and can sometimes help and sometimes can make the situation worse. While a standard antenna sends out radio waves equally in all directions in a pattern shaped like a balloon, long range antennas achieve greater range by changing the shape of the signal.

Instead of sending out the signal in a balloon shape some antennas flatten out the balloon into more of a donut, sending less of the signal straight up into the sky and more out towards the edges. These antennas can generally extend the usable range from 10% to 30%. However they can introduce two new problems; the case of the laptop seeing the hotspot but the hotspot not being able to see the laptop mentioned above, or a case where the "donut" is so flat that it shoots over the heads of the users, like a layer of fog traveling a few feet off of the ground. Generally if the property is flat, antennas with a gain of 6dbi or less are acceptable and will not shape the signal pattern to such an extent that it will introduce more problems.

A second type of antenna re-shapes the signal even more, sending it in a beam. These antennas can increase range ten-fold or more, however if the user is not in the direct path of the signal they will not be able to see it. Even if they are in the direct path if they are not able to send a signal back the full distance they will not be able to establish a connection. These high-gain point-to-point antennas are best used in pairs, one on each end of the path, and while not practical for laptops they are good for connecting buildings in remote locations or repeaters in areas not contiguous to other units.

There are other ways to improve the range of the signal for users. One way is to improve the sensitivity of the radio receiver at both ends. However we do not have control over the quality of the radio in the user's laptops.

Another way to improve range is to increase transmit power. Again, since we do not have control over the quality of the user's laptops we cannot affect their transmit power, but we could boost ours. Here where some caution is required: There are some hotspot companies that do use higher power, but that is a dangerous game. Operation at higher power can result in the property owner being fined.

*(Signal Strength, continued)* When you boost the transmit power on one end of the connection but not the other you also run into the problem of one side being able to see the signal from the other side but not being able to send a signal back.

Since laptops do not have good antennas and do not generally use the maximum output power they really benefit from having a high density signal. The best way to have a high density signal is by using multiple access points.

Determining the proper number of access points requires taking into consideration several factors: How great a distance do you need to cover? What are the surroundings? Are there walls or open spaces? Is the building made of wood, rebar reinforced concrete, or steel? Is there any interference in the area?

On a flat open field with no interference a signal can travel up to 1000'. When we start adding walls, other devices and users, that distance will begin to shrink.

For example, a hotel with two wings each 200 feet long and three floors per wing, made of rebar reinforced concrete, might need 5 units, one master and 4 mesh repeaters, to provide solid coverage. Another hotel, constructed of wood but with similar dimensions, may only need 3 units, one master and two repeaters to provide solid coverage.

Another example would be a campground that is on an open flat field. To provide complete coverage however you need to penetrate the aluminum skin of the travel coaches which might require mesh repeaters spaced every 300 feet, so that no coach is more than 150 feet from a unit.

If that hotel happens to be at the end of an airport runway with a radar system nearby or that campground has a cell tower in the middle of the property then interference from those devices may necessitate additional units to overcome the interference.

#### **Special Note on Power Levels**

The rules regarding the maximum allowable transmitted power output for 802.11 wireless data communications specify out how much energy may be used to transmit these signals. These rules cover two different types of transmissions; point-to-multipoint and point-to-point.

Point-to-multipoint is a hotspot, sending data from one or more access points to several end users.

Point-to-point is for interconnecting two buildings or areas, and is not meant to directly provide service to end users.

The allowable power levels for point-to-multipoint are lower than point-to-point. There are some hotspot vendors who use higher powered access points to compensate for having fewer access point on a property and may be confused by the rules on allowable power levels or who may disregard them altogether.

Using higher than allowed power levels can cause users to be able to "see" a strong signal from the hotspot, but not be able to get a signal back to that hotspot, causing the data session to fail.

Using higher than allowed power levels can cause excessive RF (radio frequency) noise that can interfere with other devices, such as two-way radios, cordless phones, security cameras etc.

Using higher than allowed power levels can incur fines beginning at \$5,000 per occurrence, and are the liability of the property owner.

## Glossary of Terms

*The definitions below may not be the most technically complete, but are intended to give you an understanding of what each term means in relation to providing guest Internet access.*

3G – a method for the cell phone companies to transmit “high speed” internet and data access over their networks. Very limited coverage – mostly urban areas, and expensive.

802.11 – The standard that describes how wireless devices and networks should function. Devices complying with the 802.11 standards can work with each other even if they are from different manufacturers. *Stay away from any device that is a "Pre-Standard device." These devices are rushed to market to capture sales before the final standards are released, and may end up being incompatible!*

Access Point – A “transmitter” used to connect wireless laptops and other devices to a network.

Bandwidth - The volume or amount of data that can be transmitted by a given mechanism. Dial up Internet access is considered low bandwidth because it is slow. Cable and DSL are considered higher bandwidth because they are faster. Bandwidth can also refer to the amount of data a user consumes. Some activity uses little bandwidth, such as email and on-line chat. Some activities use lots of bandwidth, such as downloading movies and watching video on line.

Broadband – A generic term for fast internet connection – generally any connection faster than dial up.

Bit – A single unit of digital information. It is either a “1” or a “0” and these bits are strung together into longer chains of numbers to represent everything on a network.

Bytes – 8 bits

Cable Modem – A modem using the Cable Company’s system to transmit data. Cable modems can be used to access the internet, and also provide telephone service in some areas. Speeds can be as high as 8Mb/second in the U.S., and up to 100Mb/second in other countries.

Captive Portal - A mechanism that captures the users web browser and redirects them to a designated web page, no matter where they try to surf to. Typically a captive portal is used to take users to a login page if they do not already have permission to use a network.

Cat 5/5e/6 – **CAT**egory 5/5e/6 cable – the cable used to connect network devices. Might look like a phone cable, but it is not.

DHCP—Dynamic Host Configuration Protocol - The process by which a router or ISP automatically assigns IP addresses to computers and other devices on the network. DHCP addresses are dynamic - they will change periodically.

Dial-up – An internet connection achieved over voice telephone line. Generally dial-up speeds are less than 32kbs (kilobits per second), and never more than 53kbs. Never, despite what marketers claim.

DSL – **D**igital **S**ubscriber **L**ine – A digital data connection that uses standard telephone wires and can be used independently of your phone line. DSL is available from some phone companies in certain areas. In order for DSL to work you must be within 20,000 feet of the phone company switch. Speeds can be as high as 8Mb/second.

Fiber Optic – A digital connection using strands of glass to bring laser powered pulses of light into a special modem (Really, we did not make this up). This technology is used in large businesses. Verizon is now experimenting with using it for home users and small businesses, under the FIBos brand. Speeds begin at 100MB/s and go higher. Can support cable TV like services.

Firewall – A device or software program used to prevent unauthorized intruders (hackers) from getting into a network or computer. Many operating systems such as Windows XP (with SP2) and Mac OSX have software firewalls built in. Devices such as routers often also have simple firewalls built in. Software is also available to add to computers to act as firewalls. *Every computer should have one software firewall installed on it, and only one. It is also a good idea to use a firewall style hardware router. More than one software style firewall on a computer offers no more protection and will degrade the performance of the computer.*

Gateway – a device connecting one network for another, for example the master unit in a hotspot system is the gateway to the internet. Hotspots are a controlled gateway, most wireless access points are uncontrolled gateways.

Hotspot—An area covered by a wireless signal. A Private Hotspot may be intended for a company or organization, and include security measures to protect the system and data. A public hotspot is an area of coverage intended for use by the general public, and usually has no security, but may require an access code or payment.

ISP – Internet service provider – a company or organization that connects end users to the internet, often by one or more means such as dial-up, Broadband or wireless. Often also provides other related services, such as email, web hosting, and even telephone services.

Kilobit – 1024 bits strung together.

Latency – The time it takes for data to get from one point to another across a network. Lower numbers are better, and express in milliseconds (thousandths of a second). Latency is very high on satellite connections because of the very long distances traveled, more than 44,800 miles to get up to the satellite and back.

Megabit – 1024 kilobits

Modem – (**M**odulator **D**emodulator) A device for connecting computers and related equipment to data networks and phone lines. Different types of modems can connect to regular phone lines, DSL lines, Cable modems, Satellite Dishes, T1- lines etc.

POE – Power over Ethernet – A way of sending power to network devices without running separate power lines.

QoS – Quality of Service – A term used to denote what type of traffic gets priority on a network. Time sensitive traffic such as voice and video might be awarded high QoS, while non-time sensitive traffic such as email and web browsing might be given lower QoS.

Router – A device to direct the flow of traffic across a network. Most devices sold as “routers” are really combination devices, often incorporating a router, a switch, a DHCP server, and sometimes an access point. It is just easier to call it a router.

Satellite – Sending data from ground stations to satellites 22,400 miles up in space and bouncing them back to a dish on your roof. Speeds can be as high as 5Mb/second, but will be slower at certain times when many users are on. Can be *much* slower. Sometimes the only choice for Broadband in rural areas.

Spam (also Spammer) – Spam is unwanted email – electronic junk mail. It is illegal in many countries to send Spam, and most ISP’s forbid the use of their networks to send Spam. *Spam accounts for over 80% of all email sent, and is a serious problem for network operators.* Because of the less than legitimate nature of Spamming, Spammers use a variety of means to send emails, including looking for unsecured wireless networks.

T-1 – A dedicated data line with a speed of 1.4Mb/second – tends to be expensive, but provides consistent bandwidth.

WISP – Wireless Internet Service Provider – An ISP using wireless technology to connect it’s users to the main network. Different from 802.11 technology, WISP’s often use non-standards- based systems that are transmitting to and from fixed points, often at lower speeds than 802.11, but at about the same speed as a typical DSL or cable modem (typically between 1 and 8 megabits). These transmissions are higher powered and are usually required by law to be licensed.

ToS – Terms of Service – The policy and rules for using a network. Your ISP may have terms of service which do not allow certain uses on their network.

WiFi – **W**ireless **F**idelity – A buzzword used to describe wireless network connections using the accepted 802.11 standards.

WEP – **W**ired **E**quivalency **P**rotection – a process to help secure the data transmitted across the wireless portion of a network. Relatively simple and not the most secure. WEP can not be used in any hotspot intended for public use.

WPA - **W**iF*i* **P**rotected **A**ccess (**WPA** and **WPA2**) – a process to help secure the data transmitted across the wireless portion of a network. More secure than WEP, but not 100% secure, can not be used in any hotspot intended for public use.

## The Checklist

Questions to consider before selecting a vendor for your Guest Internet Access.

How much will this system cost?

How much is the equipment?

How much is the installation?

Can I install it myself?

What do I need to provide separately?

How long does it take to install the system? How soon can it be installed?

What warranties are included with the system?

If I am not happy with the system can I return it?

Who provides the Internet service to the property (Who is the ISP?)

Who pays for the Internet service to the property?

What are my recurring costs? Can they be suspended in my off-season?

Does the vendor or the property owner set the pricing? Can I give access away for free to my customers? How much will it cost me if I choose to give it away for free?

What control do I have over the system?

How do users authenticate on the system?

Can I see who is on-line and how much data they have used?

Can I restrict the amount of data usage to prevent bandwidth hogs?

Can I see the status of all of my access points?

Can I log into the system remotely, from off of the property?

What support is provided for the property management and employees?

Is there live, toll-free support available?

What support is provided for the guests (and at what cost?)

Is there live toll-free support available

How are repairs handled?

Who is responsible for software updates? How is that handled?

Who else is using this system? (References)