Helping Them to Get On Line: Providing Internet Access for Your Guests

Guest Internet Access

Technical Issues, Best Practices and Definitions for Providing Guest Internet Access

CheckBox Systems LLC
www.CheckBoxSystems.net

Wireless Internet access is a staple of guest amenities and a key to a positive guest experience. No longer optional, consistent, stable wifi coverage is required by most guests across all demographics. WiFi systems that were adequate to satisfy these guests in the past may no longer keep them happy, and many properties are finding it is time to step up their systems.

Providing Internet Access DOES NOT have to be difficult or expensive. 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.

J Ganley

Jim Ganley
CheckBox Systems
www.CheckBoxSystems.net

Table of Contents

Different Ways of Providing Internet Access for your Guests

Some properties provide computers in common areas or business centers connected to the internet for guests to use. These computers should be locked down so that guests can not install software or other applications which could damage the machines and must also have strong anti-virus and security software to prevent them from downloading and spreading viruses and malware. They will periodically need to be reloaded with their software. They should be located in an area that is monitored or within view of the front desk, physically secured and a written acceptable use policy should be posted.

Providing wired high speed connections for guests to use allows you to share Internet connection(s) among your guests. These wired connections may be located in a common area, meeting rooms or distributed throughout the property. Some franchise systems will require their members to provide wired connections, often in meeting or conference areas and sometimes in guest areas. 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.

However, not all devices can use wired connections; tablets, smartphones, some gaming devices and even some laptops lack the Ethernet ports to use wired connections.

Most laptops, tablets, smartphones and other devices use WiFi to connect wirelessly to wireless access points. The range of these wireless devices vary, and can be as little as 25 feet inside a concrete building, to over 500 feet outside in a field. Wireless networking is the most cost effective way to provide high speed access, particularly in existing properties, although wireless connections can be affected by radio interference and other factors.

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. Most newer properties are all wireless, providing wireless connectivity throughout the property for their guests to use.

Should you charge for Internet Access?

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 premium locations, such as airports, where there is a captive audience with corporate expense accounts, you can still charge for internet access. But most users are unwilling to pay large amounts for access, and if they have a choice then they simply go 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 - Most people won't think twice about spending a dollar on a candy bar or a bottle of water. If you make internet access cheap enough, many guests won't think twice about buying it. Consider a pricing model such as $1.95 for one hour, $2.95 for one day, and $6.95 for one week. Few guests will ever buy 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.

"Free" - Many properties have moved to Free Internet Access. Of course it is not really free, the cost is built into the rate the guest is charged for other services or goods. 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 use 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 in with social media, 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 model.

Tiered Access - A trend among some properties is to offer tiered access. Tiered access is providing a basic level of free service and then charging for premium service. The free service is offered at a slower speed and the premium service provides for faster speeds, sometimes with the promise to provide enough speed to stream video. Properties offer tiered access for a fee or to customers who are part of a customer loyalty program.

When offering tiered access properties need to make sure that they have the system and bandwidth can that can provide a truly superior experience for the guests on the higher tier. This may mean making an investment in more bandwidth and systems with more capacity.

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 customer's 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.

What is a Guest WiFi System?

A Guest WiFi System allows your guest to easily connect wirelessly to your Internet connection while preventing unauthorized access and abuse of the system.

In order to do this the Guest WiFi System needs the ability to:
✓Differentiate between authorized and unauthorized users
✓Handle high volumes of users
✓Distribute bandwidth evenly and efficiently among users
✓Prevent users from using excessive amounts of bandwidth
✓Prevent users from engaging in file sharing or other activities that could create liabilities for the property.
✓Remove users when their time has expired

Most Guest WiFi Systems should also be able to:
✓Present a welcome page with terms and conditions of usage
✓Manage multiple Access points
✓Manage multiple ISP connections for increased bandwidth and redundancy

A Guest WiFi System should be set up outside of the company network to prevent guests from accessing the company's network. Properly set up it is possible to safely share the same Internet connections with the company network.

A home or small office WiFi router is not a Guest WiFi System, and should never be used for one.

Guest WiFi Systems should be run on business class Internet connections. These connections can be provided via fiber, cable, DSL, Satellite or other types of connections.

The terms of service for most Internet Service Providers for residential accounts forbid the sharing of the connection outside the home, and hold the account holder directly responsible for all activity on the connection. Business class Internet connections usually allow for sharing of the connection with your guests and may provide some protection from liability if the property is taking precautions to prevent abuse of the connection.

The Costs of Providing Internet Access

There are several costs involved with providing Internet Access for your guests and these costs will vary depending upon the size of the property, the volume of usage, the quality of service provided and the vendors used. Over the lifespan of a system recurring and maintenance costs will likely exceed the initial purchase cost of the system. If the property is a seasonal operation you will want to determine if any of these recurring costs can be suspended in the off season.

These costs extend beyond dollars spent and also include the value of your time and the value of the guest's experience.

It is better to know all of the costs up front before committing to a system. Some of the costs involved:

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 or other structural changes as required by the system, and lost revenue if you have to take areas out of service while installation is done. Make sure you understand what your vendor will provide for installation and what you will be responsible for. 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, insured and licensed for your location for the work that they do perform..

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 vendor's headquarters or in the "cloud" somewhere, 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.

Over time you will need to plan on updating your system and increase the bandwidth available as guest usage grows.

ISP Service - The ISP (Internet Service Provider) is the company that actually brings the internet connection onto the property (such as AT&T or Comcast). 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 (and include a vendor mark-up).

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. If you are part of a franchise system you may find that your vendor requires you to provide guest support.

Time Costs - How much effort and time you and your staff need to expend to setup and manage your guest wifi solution should also be a consideration. Some WiFi solutions can be installed by the property, which may cost some staff hours but will greatly save on installation costs. This also can have the added benefit of the property staff being more familiar with the system and make troubleshooting easier, quicker and ultimately less expensive.

How much effort will management and staff need to expend to run and manage the system is also another time cost to consider. Getting references from other users of a vendor will give you the best perspective on what is involved with daily operation.

Controlling Guest Access

There are several aspects of Internet access for your guests that you need to exercise control over, such as 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.

Uncontrolled access to your system can also lead to some guests downloading pirated movies and music and leave the property open to copyright liability issues.

If you are providing wireless Internet access, 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, consuming bandwidth, slowing down access for your guests and even exposing you to liability.

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 your Internet access for free. Most access control systems include a captive portal that 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 moderate amounts of bandwidth, checking their email, browsing web pages or posting to social media. A small minority of users will consume very large amounts of bandwidth, trying to stream movie or music, 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 to ensure that no one user is using excessive bandwidth for abusive purposes.

If you are using a metered Internet service (such as most satellite providers and increasingly some DSL and cable providers), one that only provides a set a mount 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 device, but they need to get a signal back to the hotspot. The WiFi radios in users devices 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 on their device but have a difficult time maintaining a connection. This is usually a case of the device seeing the signal from the Hotspot but the Hotspot not being able to see the device.

Users often encounter issues interpreting the signal strength displayed on their screens. These signal displays are an approximation of the signal strength averaged over a period of time and do not take into account signal noise and the interference inherit in every radio transmission. Because of factors beyond raw signal strength users may see a strong signal but are still not able to establish a connection.

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

One way to improve the range of the signal is by adding a long range antennas to your system. Long range antennas are rated in "dbi" and can sometimes help, but can also 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, these antennas flatten out the signal 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; instances of the guest's device seeing the hotspot but the hotspot not being able to see the guest's device, or a case where the "donut" is so flat that it shoots over the heads of the users, like a layer of fog traveling high above 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 guest's devices 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. Unfortunately we do not have control over the quality of the radio in the user's devices.

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

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 user's devices usually do not have good antennas, and do not generally use the maximum radio output power to save battery life, 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, interference and noise from other devices and users, that distance will begin to shrink.

For example, a hotel 200 feet long and three floors, made of rebar reinforced concrete, might need 8 access points or more to provide solid coverage. Another hotel, constructed of wood but with similar dimensions, may only need 6 access points to provide solid coverage.

Another example would be a campground that is on an open flat field. To provide complete coverage you need to penetrate the aluminum skin of the RVs which might require access points spaced every 200 feet, so that no RV is more than 100 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 facilities may require additional units to overcome the interference.

! A 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 points on a property, and may be confused by the rules on allowable power levels or may just disregard them altogether.

Using higher than allowed power levels can cause users to be ale 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*, not the vendor.

How Much Bandwidth is Enough?

A good rule of thumb is to provide at least 1 Mb/s of bandwidth for each guest when possible.

When providing Internet access for your guests one consideration is how much bandwidth is needed. Bandwidth is the measure of the maximum amount of information that can be transmitted per second, and is often expressed as megabits/second (Mbs).

With evolving usage, the amount of bandwidth used by a guest has increased dramatically. What was adequate five years ago is not sufficient today. When combined with the additional factors of larger percentages of guests using Internet services and guests carrying multiple devices the demands on your bandwidth has sky-rocketed.

A good rule of thumb is to provide at least 1 Mb/s or more of bandwidth per guest when possible. For a 100 room hotel with 2 beds in each room, that is potentially 200 guests, or 200Mb/s. For a 40 seat coffee shop plan on 40Mb/s. This is a case where more is definitely better.

At some locations adequate bandwidth may not be available. In some cases multiple ISP connections may be used to provide more bandwidth, and you may need to limit the speed or amount of access your guests receive. Make sure your system is capable of using multiple connections and limiting users as necessary.

Different technologies provide different amounts of bandwidth, and the performance of these connections will vary by provider, your local area, and even by time of day:

Web browsing, email and even watching video is mostly a downloading affair – the guests are pulling down data, and the upload is just a request for the data. Some applications such as voice and video chat require good upload speeds as well as good download speeds.

Technology	Typical Download Speeds
Satellite	Typically less than 1Mb/s, upto 20Mb/s
DSL	From less than 1Mb/s up to 25Mb/s
T1	1.44Mbs
Cable	2Mbs to 1,000+Mbs
Fiber	20 Mbs to 1,000+Mbs

Most Internet Service Providers provide download speeds faster than the upload speed. The ratio of download speed to upload speed will vary.

In many areas it is not unusual to have limited access to bandwidth, or bandwidth may be very expensive. If that is the case and you are limited to the bandwidth you can provide guests you may need to restrict usage, possibly by providing a limited amount of time guests can be on-line, or by charging guests to discourage casual usage.

How much bandwidth is consumed by different activities?

Activity	Typical Consumption
Sending/receiving email (no attachments)	.001Mb
Sending/receiving email w/ 1 picture	1.5Mb
Downloading a 3 minute song	5Mb
10 minutes on social media	20~50Mb
Streaming a 3 minute video in HD	180Mb
Using Skype for a 20 minute voice chat	4~10Mb
Using Skype a 20 minute video chat	40~60Mb
Watching a streaming 30 minute TV show	400~600Mb
Watching a streaming 2 hour movie	1800~4000Mb

A two hour movie can be the equivalent amount of bandwidth of over
4 million emails!

Choosing an Internet Service Provider (ISP)

When it is time to select or increase Internet bandwidth for your guest Internet access know that ISPs have very different packages, pricing and technology. If you are lucky enough to have a choice of providers take the time to contact every ISP that serves your area and get quotes. In many cases you can negotiate on pricing and terms if there is competition, especially if you bundle services such as phone and TV, although in some cases bundling may not give you the best prices or service.

Prices, plans and promotions change often and it is a good idea to shop around every year. In some cases you may find that there are no providers that can provide you with a connection that has enough bandwidth to adequately serve your guests. However some WiFi vendors have equipment that can use multiple connections to get more total bandwidth for your guests. It is not unusual for larger properties in areas with limited ISP service to use several or even dozens of connections to serve their guests.

For example, if your have a local DSL provider that can only provide 6Mb/s of bandwidth per modem (circuit), if your WiFi vendor's equipment can handle it you can order multiple 6Mb/s circuits from the ISP and use them to prove more total bandwidth to your guests.

Even if your ISP can deliver adequate bandwidth on a single circuit, if your WiFi Vendor's system can handle multiple connections to ISPs, consider adding additional connections from a different ISP if available. With a connection from two different ISPs you not only have more total bandwidth for your guests, you also have redundancy for when one of the ISPs has problems and goes down.

Speed vs. Bandwidth

The bandwidth of your Internet connection and the speed of the connection are related, but not the same thing.

Bandwidth refers to how much data your Internet connection can deliver and is usually measured in megabits-per-second. A 1Mb (one-megabit) connection can deliver just over 1 million bits of data per second.

Speed is how quickly those bits of data get to you, and is measured in milliseconds. Speed is affected not only by the bandwidth of your connection, but also by how many users are using it, what those users are doing, how well connected your Internet Service Provider is to the rest of the Internet, as well as congestion on the Internet and the capabilities of the web service that the guest is trying to access.

If your ISP delivered hot water instead of data, then the bandwidth of your bathroom would determine if the shower was a trickle of water or if it was a deluge. And the speed would be how long it would take from when you turned on the hot water until it actually got good and hot. As with Internet, the quality of the shower can be affected by other users of hot water in the house and by the showerhead itself.

Internet connections that have the same or similar bandwidth ratings may be very different when it comes to how responsive and stable they are.

Meshing and Point-to-Point Networks

The fundamental purpose of a network is to connect together two or more things. In a computer network we connect computers and related equipment.

Network layouts and connections fall into two very broadly defined categories: Point-to-Point and Meshed.

The vast majority of network connections are point-to-point. Think of a desktop PC plugged with an Ethernet cable to a router which is plugged in with an Ethernet cable to a modem which is connected by a coaxial cable to the cable network. In this scenario each device is connected to the next point in the network by a single pathway, and if any of those pathways fail, the connection fails.

In a mesh network each device (we will call it a node) has multiple connections and each node is designed to be aware of all of its potential pathways. If one pathway is lost the node will instantly flip to another pathway.

Meshing is used in core routing functions in large networks, with the Internet being the classic example. These large network routers keep routing tables for all of the possible routes to get from here to there, and they also track the cost of the route (cost defined as efficiency as well as the actual dollar cost of transiting data across links that are metered).

In the early days of networking these routers would need to have their paths and cost set up manually. Eventually protocols and mechanisms were developed to allow routers to communicate to directly to determine the best paths. As a result of this automatic discovery and sharing routers are constantly updating their routing tables, often hundreds or thousands of times per second.

Some wifi companies use point-to-point connections to feed their access points. (Point-to-point is also known as bridging). In a point-to-point setup one connection is made between the access point and it's connection. In a point-to-point scenario there is no alternative path or fallback and when that point-to-point connections becomes heavily loaded, degrades, or fails the access point (and guests using that access point) suffer. Point-to-Point systems require someone with networking knowledge to set up the initial routes, set IP addresses, SSIDs paths etc. for each and every access point and point-to-point bridge.

More advanced wifi networks will use meshing instead of point-to-point. Advanced meshing protocols are designed to allow the mesh nodes to automatically discover each other, setup links and constantly update each other to be aware of routing conditions and alternate pathways. The only action required of the system operator is to accept the mesh node into the mesh. The implementation of automatic meshing protocol results in a more robust system and lower cost of implementation.

One misconception is that meshing, "cuts the bandwidth in half for each hop".

It is not as simple as that.

If in a mesh architecture you have a single radio picking up packets from one source and then relaying them to another source, and that radio is simplex (i.e. it can only send or receive, but cannot do both at once) then that is a valid criticism. Point-to-point networks experience the same halving of the bandwidth that will occur unless you are using multiple radios at each location.

To further complicate the issue in a network there are many factors that determine total bandwidth or throughput. These include the capabilities of the network hardware, the signal strength and the ambient radio noise at the access point, the ambient radio noise and signal strength at the upstream connections serving the access point, the ambient radio noise and signal strength at the user devices and the capability of the users device, as well as total bandwidth available to the property and current client load.

With all of those factors combined, in a point-to-point network any issue will have a major impact on network performance and user experience, with no options to fall back on.

In a mesh network if there is noise or interference at a mesh node's upstream connection then the mesh node can re-route instantly if the mesh is properly built.

In a perfect lab environment a point-to-point network may perform better. In a real world environment a properly built mesh network will always perform better and will be still be serving users when the going gets tough.

There are times when a dedicated link is needed to get extra bandwidth out to far flung locations. These links can be meshed or point-to-point, again with meshed links being more reliable.

In addition to more reliable network performance mesh networks greatly enhance the ability to trouble shoot problems; often when one member of the mesh is experiencing issues or fails other members of the mesh that are still functioning are able to provide important feedback about nearby noise and signal conditions.

Glossary of Terms

These definitions 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/4G/LTE – a method for the cell phone companies to transmit internet and data access over their networks. Limited coverage – more available in populated areas, and expensive. Often comes with limits on usage with expensive overage charges.

802.11 – The standard that describes how WiFi devices and networks should function. Devices complying with the 802.11 standards can work with each other even if they are from different manufacturers.

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

Asynchronous - Refers to a data connection where the download speed and upload speed are not equal. Typically the download speed in an asynchronous connection will be several times more than the upload speed.

Bandwidth - The measure of the maximum amount of information that can be transmitted per second, and is often expressed in megabits/second (Mb/s). This is also referred to as the speed of the Internet connection, although this is often a misleading indicator of speed. Some activities 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 a fast internet connection.

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 1000Mb/second in the U.S.

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. Looks like a fat phone cable.

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. Very slow.

DSL – **D**igital **S**ubscriber **L**ine – A data connection using 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.

Fiber Optic – A digital connection using strands of glass to bring laser powered pulses of light into a special modem. Speeds begin at 20Mb/s and go to over 2,000 Mb/s.

Firewall – A device or software program used to prevent unauthorized intruders from getting into a network or computer. Many operating systems such as Windows and Mac OS 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 a 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 requires an access code, accepting terms of use or payment.

IP Address - The unique numerical address used to identify a device on a network. These addresses are usually not permanent and can change often.

ISP – **I**nternet **S**ervice **P**rovider – 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 expressed 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. Latency can greatly affect how fast an Internet connection "feels".

Megabit – 1024 kilobits

Modem – (**Mo**dulator **Dem**odulator) 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, satellite dishes, T1- lines etc.

PoE – Power over Ethernet – A way of sending power to network devices over existing network cables 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 to consumers as "routers" are really combination devices, often incorporating a router, an Ethernet switch, a DHCP server, a firewall, and sometimes a WiFi access point.

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 20Mb/ second or more, 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 then legitimate nature of Spamming, Spammers use a variety of means to send emails, including looking for open 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. WISP's often use non-standards- based systems that are transmitting to and from fixed points, at about the same speed as a typical DSL or cable modem (typically between 1 and 20 Mb/s).

ToS – Terms of Service – The policy and rules for using a network. For example, your ISP may have terms of service which do not allow certain uses on their network. You should have a posted Terms-of-Service for your guests to use your 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 a hotspot intended for public use.

WPA - **WiFi Protected Access** (**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 a 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 *in total*?
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 for users? 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? (Get references)