INNOVATOR IN ELECTRONICS

White Paper

WaveBolt™ System Discription

Murata Electronics, North America

Table of Contents

WaveBolt

The WaveBolt™ system is a fixed wireless point-to-multipoint Internet access system designed specifically for residential and small business customers in areas where DSL and cable modem access are unavailable, unaffordable or otherwise undesirable. The WaveBolt system provides data speeds comparable to ADSL. Simple to install, the WaveBolt CPE in many cases will be installed by the end user. And, where customers choose to have the CPE installed, a single, short site visit is all that is required to complete the installation.

There are two versions of the WaveBolt system: Series 9 and Series 58. Both of these WaveBolt systems provide 1.05 Mbps of data throughput. The Series 9 product operates in the 2.4GHz frequency band. Series 58 operates in the 5.8 GHz band.

The WaveBolt system is comprised of an Access Point (AP) and an Access Point Radio (APR) located at one or more Points of Presence (PoPs) of the ISP and CPE or Subscriber Unit Equipment (SU) located at the subscriber's location. The access point is connected to the ISP network to gain access to the Internet. The CPE is connected to the subscriber's PC through a USB connection or an Ethernet connection.

Summary of System Functionality

- Point to multi-point last mile access network (star topology)
- 5 mile range in the U.S. and most other countries; 3 kilometer range in E.U. regulated countries
- Non-line of site performance in near range to access point
- 1.08 Mbps aggregate data rate per access point radio sub network
- 60 subscribers maximum per access point radio sub network
- Scalable from one sub-network (60 active subscribers) to 20 sub-networks (1200 active subscribers) per point of presence
- TCP/IP protocol based
- Ethernet, USB and serial interfaces available for subscriber units
- Frequency hopping spread spectrum access scheme
- TDMA modulation
- ISP network management and control, RADIUS and SNMP support
- System diagnostic and planning tools

WaveBolt System Features

- **Frequency Planning Utilities** – When planning a network deployment, operators can gather data on a per channel basis to determine the optimal hopsets, (i.e.: those that avoid interference), to select for a given sub-network
- **Optimized Frequency Hopping** – A wide range of frequency hopsets can be selected and utilized in order to avoid congested areas of the spectrum
- **Radios Synchronization** – Radios can be synchronized so that they transmit and receive at the same time thereby eliminating a potential source of interference
- **Frequency Hopping Spread Spectrum (FHSS)** – Radios hop from channel to channel thereby avoiding interference
- **TDMA Performance** – Greater network throughput in high duty cycle usage periods.
- **Fixed Modulation** – All subscribers in a sub-network will be allocated equal bandwidth given unimpeded line of sight and lack of interference.
- **Non-Line of Sight Performance** – Subscribers close to the access point (<1 mile) can get coverage even when not in direct line of sight of the access point.
- **Quality of Service via Maximum Data Rates** – Users data rates can be capped affording bandwidth management
- **RADIUS Server Support** – Networks can interface with ISP's Radius servers allowing comprehensive authentication, accounting and administration functions.
- **Robust System Security** – Inherent security in FHSS scheme as well as radio and IP security fuctions.
- **Modular Architecture** – The system can be expanded incrementally by adding access point radios and cards only when necessary, minimizing initial capital investment.
- **SNMP Based Network Management** – Full configuration, control and monitoring is available through SNMP
- **USB, Ethernet and Serial Subscriber Connectivity** – Maximum flexibility for ISP subscribers.
- **Adjustable Upload/Download speeds** – Bandwidth can be configured for characteristics of the network traffic.
- **Easy to Install Integrated Subscriber Unit** – Subscriber units are compact and easy for the end user to install thus eliminating the need for a complicated installation.

The WaveBolt System

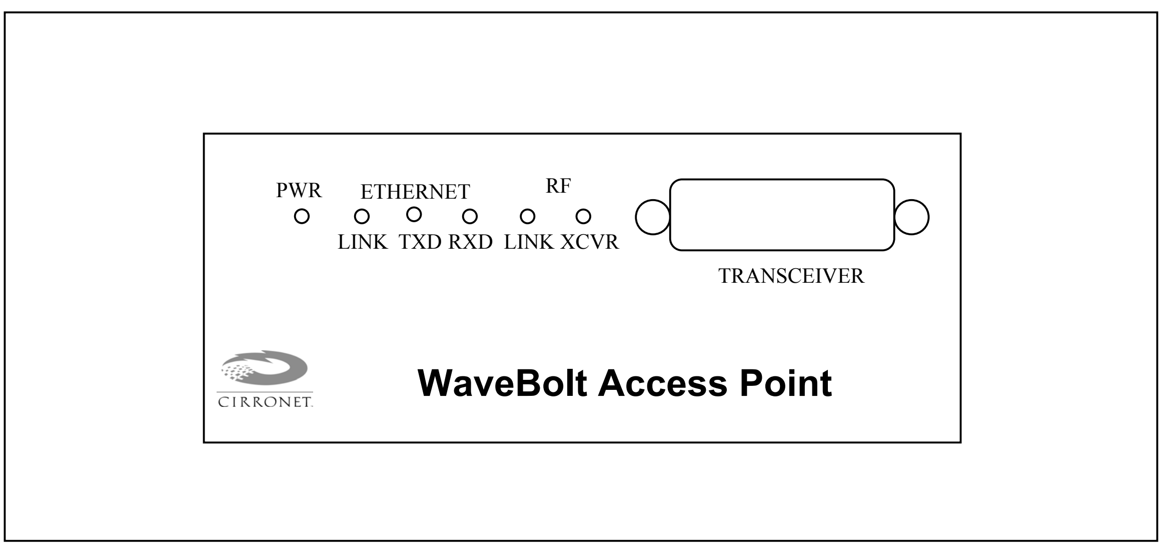
WaveBolt Access Points

The WaveBolt family has two different access points allowing optimal system design regardless of the number of subscribers to be served. The WaveBolt access points are the WaveBolt stand alone access point (WBAPSA) and the WaveBolt card cage access point (WBAPCC). The WaveBolt stand alone access point and WaveBolt card cage access point can be used with Series 9 and Series 58 SUs.

Because many times the connection between the access point and the network is located some distance away from where the access point antenna needs to be located, for example, on top of a tower, long coaxial cable runs carrying the Radio Frequency (RF) signal are needed. Coaxial cable is expensive, difficult to install and creates loss in both the transmitted and received RF signals or requires the use of expensive amplifiers. To avoid this cost and loss of performance, the WaveBolt system was designed so that the WaveBolt Access Point Radio (WBAPR2/9/58) is installed near the access point antenna, typically on a tower or on top of a building. This allows for the use of up to 500 feet (150 meters) of standard multi-conductor cable. The WaveBolt access point radio assembly comes with a mounting bracket to attach it to a tower or building top and includes a short 2-foot (0.6 meter) length of low loss RF coaxial cable. The mounting bracket has mounting holes to mount the antenna.

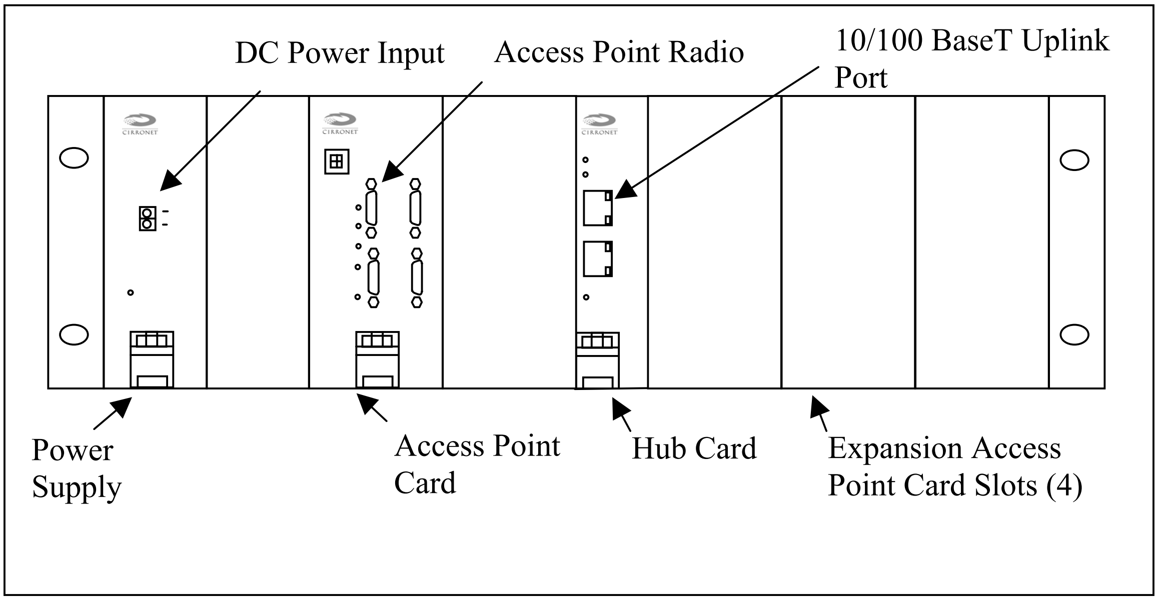
The WaveBolt Stand Alone Access Point

The WaveBolt WaveBolt stand alone access point is a low cost access point designed to serve up to 60 Series 9 or Series 58 simultaneously active subscribers. Contained in an aluminum enclosure, the WaveBolt WBAPSA supports 10 and 100BaseT network connections. The WaveBolt WBAPSA is rated over a -30° C to +70° C operating temperature range allowing deployment without heating or cooling. Expansion of WaveBolt WBAPSA PoPs is accomplished by adding additional WaveBolt WBAPSAs.



The WaveBolt Card Cage Access Point

The WaveBolt card cage access point is a standard 19-inch 3U high rack-mount card cage. The WaveBolt access point card, which is installed in the card cage, performs the work of transferring data back and forth from the Internet to the subscribers. The access point card is connected to the ISP network through a 10/100BaseT connection made to a WaveBolt Hub card, also installed in the card cage. A power supply card that converts +/- 48 volts DC into the voltages necessary to power the access point card and the Hub card completes the base card cage configuration. Each access point card can support 4 access point radios, each of which can support 60 simultaneously active subscribers, for a total of 240 simultaneously active subscribers per access point card. As the card cage can accept 5 AP cards, each card cage can support up to 1200 simultaneously active subscribers.



Access Point Features and Functions

In addition to the core function of sending and receiving data from subscribers to and from the Internet, the WaveBolt access points can perform other functions that simplify the installation and management of a WaveBolt system.

Authentication

The WaveBolt access points have the ability to authenticate users as they log on using a username and password scheme. If the access point is to perform authentication, the default, a username and password in entered for each user. When the subscriber connects, the username and password the subscriber enters must match the username and password stored in the access point. The access point can accept multiple log-ins of the same username and password although the default is to allow only single log-ins.

The WaveBolt access points also support RADIUS authentication, both CHAP and UPAP. In this instance, the access point receives the username and password information from the subscriber and passes it on to the designated RADIUS server which will perform the authentication.

In WaveBolt systems is using the WaveBolt card cage access point with multiple access point cards installed, it is possible to have one access point card act as a master authenticator. Under this scheme, all usernames and passwords are entered in the master authenticator access point card. The other cards are set up to feed authentication information to the master authenticator which performs the username and password verification and check and returns the results to the requesting access point card.

IP Address Assignment

When a subscriber logs on to the access point an IP address is assigned to that subscriber. There are three ways that assignment can be performed. A RADIUS server can be specified to assign IP addresses or the access point can assign the IP addresses in one of two ways.

The default access point IP address assignment is a sequential assignment based on a starting IP address. This base IP address is entered into the access point. The first subscriber that logs onto the access point receives the base IP address. The second subscriber to log on is assigned the next higher IP address; the third subscriber is assigned the next IP address and so on. This IP address assignment is dynamic in that when a subscriber logs off the IP address assigned to that subscriber is released and can be assigned to another subscriber. When the original subscriber logs back on, a different IP address can be assigned.

The second mode of access point assignment of IP addresses is static IP assignment. In this mode, a specific IP address is specified for a particular subscriber. When that subscriber logs on, the same IP address will always be assigned. Static IP address assignment can be specified for some subscribers while the IP addresses for the other subscribers are dynamically assigned.

Network Management with Full SNMP Support

WaveBolt systems feature network management with full Simple Network Management Protocol (SNMP) support. Through SNMP, network administrators can configure access points, add, delete and manage subscribers, monitor network traffic and catch traps and alarms. WaveBolt's Network Management System has the following features:

- Easy to use command line interface
- Remote control and status through password protected telnet or a console port
- Built in DNS, RADIUS and DHCP servers
- RADIUS authentication using CHAP or UPAP
- Firmware upgrades through FTP
- Radio Synchronization in time and frequency which allows for interference free co-location
- Standard and private MIBs

RADIUS Server Support

The WaveBolt access points support RADIUS servers for authentication and accounting with each function individually selectable. That is, a RADIUS server can be specified for accounting but the access point can still perform authentication. If accounting information is desired, a RADIUS server must be used as the access point does not have any native accounting functions.

Telnet Sessions

The WaveBolt access points support remote configuration and management through Telnet sessions to the command line interface of the access point. (This command line interface is also available through a serial console port located on the access point) To prohibit unauthorized users from Telneting into the access point, a Telnet password is required. In addition, Telnet sessions are only allowed from a maximum of 5 IP addresses. These IP addresses are entered into the access point. If a Telnet session request originates from an IP address not on the list, the Telnet session will be refused.

FTP

The WaveBolt access points support FTP sessions for the purpose of storing and retrieving access point setups on remote servers. This feature allows all access point configuration parameters as well as usernames and passwords to be stored on a remote server. If an access point card is replaced, the file can be sent to the new access point card and the information will be entered automatically. The data in this file is encrypted and cannot be read or displayed. FTP is also used to perform access point firmware upgrades. Similar to the Telnet sessions, the FTP sessions are password protected and can be initiated only from specified IP addresses.

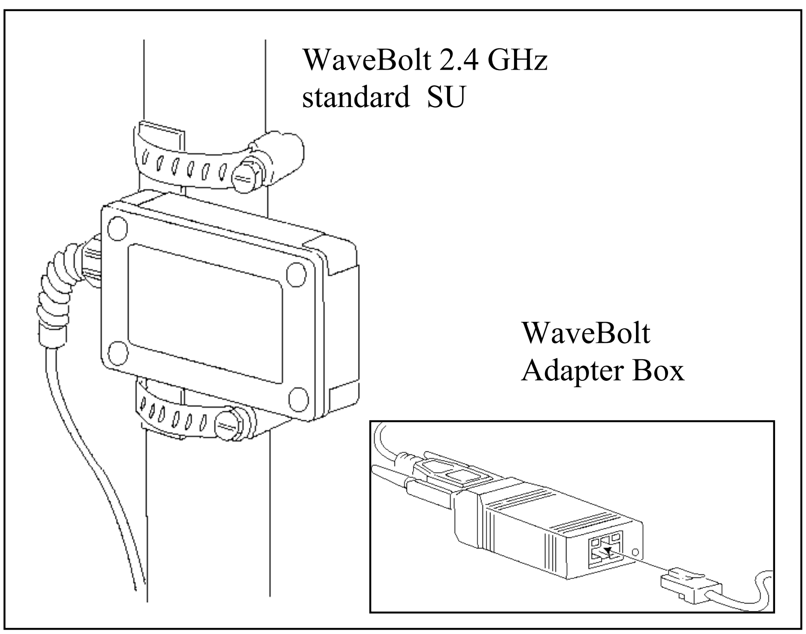
The WaveBolt Subscriber Unit

The WaveBolt Subscriber Unit (SU) is comprised of an outdoor weatherproof RF modem and radio with built-in antenna and an indoor USB adapter box or Ethernet adapter box. The RF modem has a 50-foot (15 meter) cable permanently attached to it which is run from the outdoor RF modem location to the indoor adapter box location. The RF modem comes in two styles, one with a built-in 6 dBi antenna and one with a built-in 12 dBi antenna (called a high-gain subscriber unit). The USB adapter box connects to a USB port on the subscriber's PC by means of a USB cable which is included with the SU. The Ethernet adapter has a short CAT5 cable pigtail which is connected directly to a subscriber's Ethernet port or to a router if multiple PCs are to be networked to the SU.

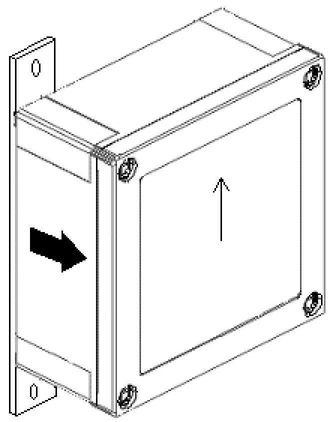
The weatherproof RF modem is enclosed in a hand-size box and is typically mounted on a roof where line-of-sight to the access point antenna is available. The RF modem has mounting flanges that can be secured to the side of a structure, such as a chimney, with two screws, or more often, secured to a short pole by means of two hose clamps which are included. The RF modem has a built-in wide-angle antenna. When the RF modem is mounted, it is simply pointed in the direction of the access point antenna. Since the beamwidth of the antennas is wide, there is no need for special equipment or precise aiming of the antenna as is needed with a satellite TV dish. Mounting the RF modem and running its cable inside is similar in effort to mounting a television antenna.

The RF modem cable is similar to CAT5 Ethernet cable and has a RJ-45 connector on the end that plugs into the adapter box. A 50-foot extension cable is available to extend the total length to 100 feet.

The USB adapter box is about one-half the size of a deck of cards. The Ethernet adapter box is about the size of a small Ethernet hub. Power is provided by a wall-mount power supply that plugs into the adapter box. Power is supplied to the outdoor RF modem



through the adapter box and the RF modem cable. The USB adapter box connects to a USB port on the subscriber's PC eliminating the need to open the subscriber's PC to install any cards. Similarly, the Ethernet adapter box connects to a PC's Ethernet port or to a router.



WaveBolt 2.4 GHz high-gain and 5.8 GHz SU

Network Requirements

The first thing the service provider needs is a connection to the Internet. Depending on the service provider’s size, this connection may be through a large wholesaler such as UUNET or through smaller, regional wholesalers. For existing service providers, the connection being used for their existing customers, whether these customers use dial-up or some other method of connection, will suffice. Typically, this connection is provided through one or more T1 or faster connections connected through a router located at the service provider’s location. Associated with this connection are one or more public IP addresses that will be assigned to the service provider. Because there are a limited number of public IP addresses available, there is a charge to be assigned a public IP address. Wholesalers may impose a limit to the number of public IP addresses they will make available to service providers based on the number of subscribers being served.

At a bare minimum, the service provider will need only the router, an access point and an access point radio. In this situation, the wholesaler for the Internet connection will also provide the Directory Name Services (DNS) and, if offered, subscriber home page hosting and mail service. The prospective service provider should contact the wholesalers to determine the various offerings available.

A typical service provider will have their own DNS and mail servers that allow them to offer home page hosting and mail services directly. The tradeoff is the cost of the additional servers and software versus the additional revenues due to the additional services being provided without the use of the wholesaler. Many service providers will have a RADIUS server as well. A RADIUS server provides a standard system for managing subscribers and their usage as well as being able to tie into billing systems.

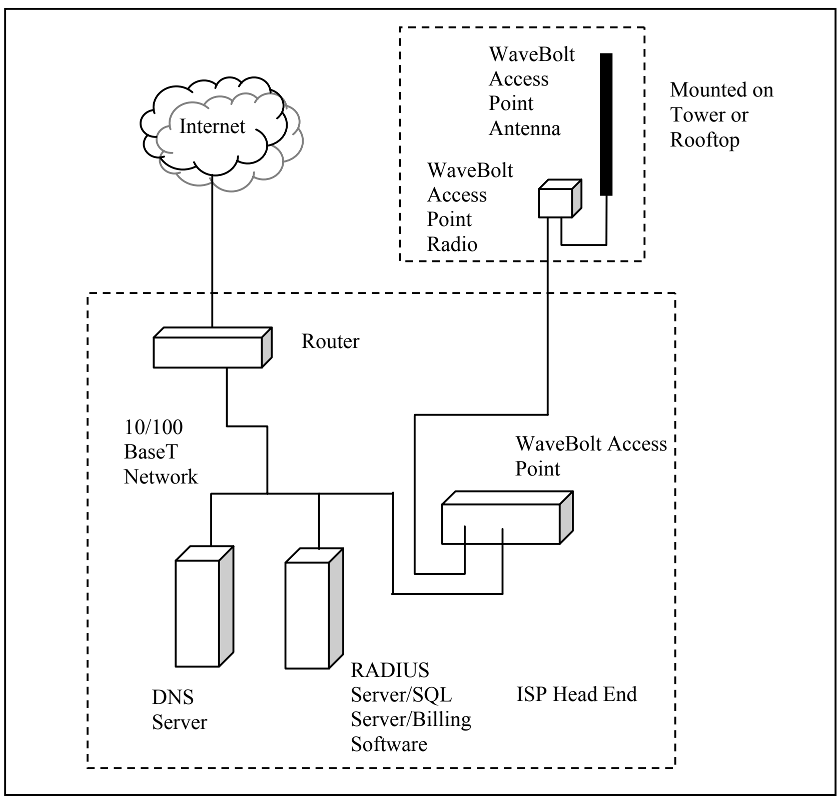
IP Addresses

In the Internet Protocol (IP) world, IP addresses are the means to direct data between locations on the Internet. Thus every device and user that is connected to the Internet must have a unique IP address. Therefore the router and the access point need IP addresses as do all of the subscribers. As mentioned above, there are a limited number of public IP addresses for the entire global Internet, a little more than 4 billion addresses. To get around this limitation, private IP addresses and Network Address Translation (NAT) are used. The router at the service provider location must have a public IP address to be “seen” on the Internet. The devices on the other side of the router can use private IP addresses. Private IP addresses are never seen by the Internet and therefore do not need to be unique from any other IP addresses used by someone outside the service provider’s network. NAT maps these private IP addresses into the public IP addresses. NAT is performed by the router connected to the Internet. Not all routers are capable of performing NAT, so it is important that capability be specified when buying the router. There is also a limit to the number of private IP addresses that can be mapped into public IP addresses. This must be considered when determining how many public IP addresses to buy.

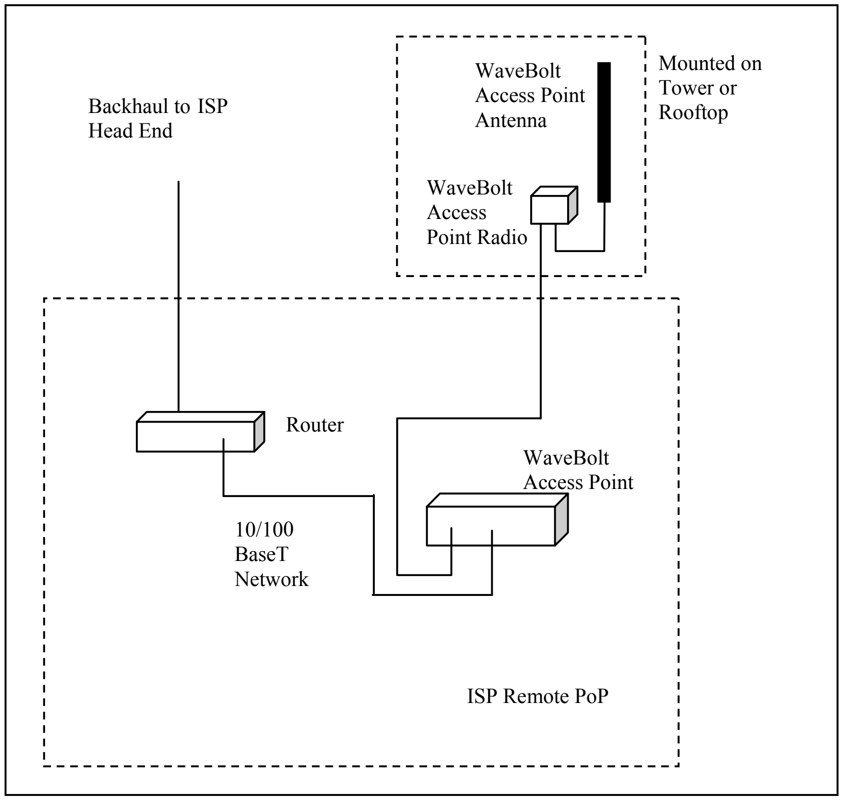
The service provider must reserve a group of private IP addresses that can be assigned to subscribers. Each access point also requires an IP address. In a typical dial-up environment there are more subscribers than there are phone lines and thus not all subscribers can be logged on at one time. In this situation, there is no need to have an IP address available for every subscriber. Rather a group of IP addresses, equal in number to the maximum number of subscribers that can be logged on at one time, are assigned to subscribers as they log on. When the subscriber logs off, that IP address is freed up for use by another subscriber. With the WaveBolt system, always on connectivity is available. In this case every subscriber can be logged on at the same time and the number of IP addresses must be equal to the number of subscribers.

Some subscribers may want to have the same IP address every time they log on. While this is not the default case, the WaveBolt access point can support this “static” IP assignment. Subscribers who are interested in playing web-capable games with other people using a different service provider, will want a public IP address. Static IP assignment, or the assignment of a public IP address to a subscriber is typically an additional charge to the subscriber.

The figure below shows a typical WaveBolt setup at an ISP head end PoP.



The figure below illustrates a typical WaveBolt setup at a remote PoP.



RF Considerations

WaveBolt system radios operate in the 2.4GHz and 5.8 GHz license-free bands. Thus they can be deployed without acquiring a license or otherwise coordinating frequency usage with the FCC or any other regulatory or governmental authority. To achieve the maximum range of 5 miles (8 kilometers), there needs to be clear line-of-sight between the access point antenna and the outdoor RF modem of the subscribers. Line-of-sight means that if a person places their eyes at the level of the subscriber unit RF modem, they can see the access point antenna without having to look through trees or foliage (obviously, for five miles, binoculars might be required to actually discern the access point antenna). As trees and foliage attenuate the RF signal, if they are in the straight path between the access point antenna and the subscriber RF modem, the range will be reduced. How much the range will be reduced depends on how much foliage is in the way. Typically, ranges between one-half mile and one mile (0.8 to 1.6 km) can be obtained without line-of-sight.

In some circumstances where line-of-sight is not available but there are other structures nearby that have line-of-sight with the access point antenna, the RF signal from the access point antenna can bounce off the structures and be reflected to the subscriber RF modem. The WaveBolt system is able to operate successfully in this type of environment. The problem is it is very difficult to predict when the geometry of the situation will properly reflect the signal. In these cases, a site survey is required. Site survey kits are available for purchase from Cirronet and are strongly recommended as an RF planning tool.

The easiest way to achieve the largest line-of-sight coverage area is to have the access point antenna elevated as high as possible. This has the RF signal path shooting over foliage rather than through it. For best results in deployments where there are hills or a lot of trees, the access point antenna needs to be positioned on a tower or tall building. In areas where the landscape is flat and without a lot of trees, less elevation is required.

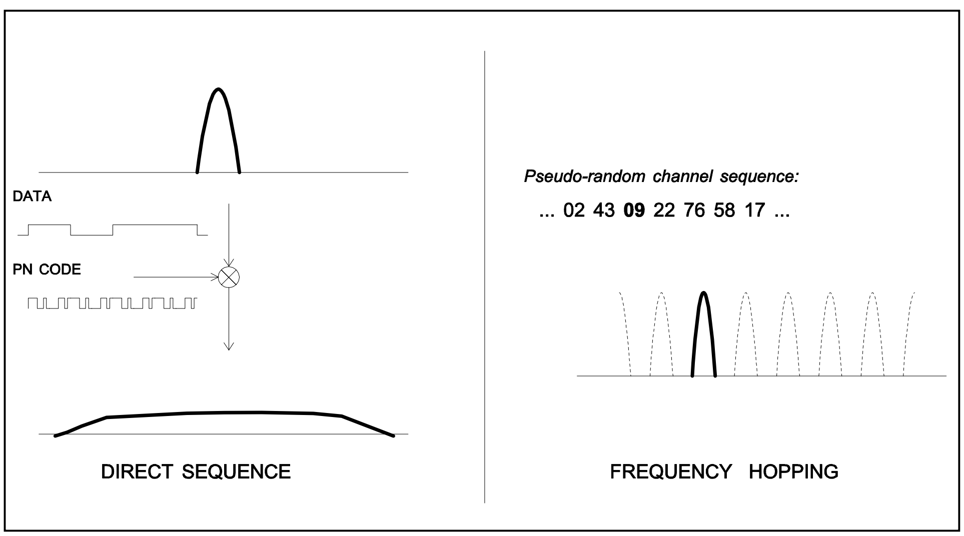
It is important to do a site survey in an area before actual deployment begins. This can be done by setting up temporary access point at the proposed site of the permanent access point. WaveBolt has a utility called RFLinkscope that measures the percentage of data packets that are successfully sent or received at a subscriber location. Using a subscriber unit, a laptop computer and RFLinkscope the area around the access point can be surveyed. Areas of high throughput can be plotted on a map around the access point and the relative merit of the location can be determined. Cirronet has a site survey kit that contains all of the necessary components to conduct an effective site survey including a temporary access point, a subscriber unit, rechargeable battery packs, RFLinkscope and a manual.

WaveBolt also features the ability to gather user statistics to determine the optimum hopset for a given user. Each of the 43 Series 9 or 75 Series 58 channels is tested to determine whether or not the channel is blocked. Extrapolating this data over a number of subscribers allows the radio link to be optimized by choosing the most advantageous hopset or by moving a subscriber to another radio or sector. An overall throughput value is calculated and can be used to look for performance improvements after optimization.

Frequency-Hopping Technology

The radio transmission channel is very hostile, corrupted by noise, path loss and interfering transmissions from other radios. Even in a pure interference-free environment, radio performance faces serious degradation through a phenomenon known as multipath fading. Multipath fading results when two or more reflected rays of the transmitted signal arrive at the receiving antenna with opposing phase, thereby partially or completely canceling the desired signal. In the frequency domain a multipath fade can be described as a frequency-selective notch that shifts in location and intensity over time as reflections change due to motion of the radio or objects within its range. Spread spectrum reduces the vulnerability of a radio system to interference from both jammers and multipath fade by distributing the transmitted signal over a larger region of the frequency band than would otherwise be necessary to send the information. This allows the signal to be reconstructed even if part of it was lost or corrupted in transit.

The two primary approaches to spread spectrum are direct sequence (DS) and frequency-hopping (FH), either of which can generally be adapted to a given application. Direct sequence spread spectrum is produced by multiplying the transmitted data stream by a much faster, noise-like repeating pattern. The ratio by which this modulating pattern exceeds the bit rate of the baseband data is called the processing gain, and is equal to the amount of rejection the system affords against narrowband interference from multipath and jammers. Transmitting the data signal as usual, but varying the carrier frequency rapidly according to a pseudo-random pattern over a broad range of channels produces a frequency-hopping spectrum system.



Direct Sequence and Frequency-Hopping Diagrams

One disadvantage of direct sequence systems is that due to spectrum constraints and the design difficulties of broadband receivers, they generally employ only a minimal amount of spreading (typically no more than the minimum required by regulatory agencies). For this reason, the ability of DS systems to overcome fading and in-band jamming sources is relatively weak. By contrast, FH systems are capable of probing the entire band if necessary to find a channel free of interference. Essentially, this means that an FH system will degrade gracefully as the channel becomes noisier, while a DS system may exhibit uneven coverage or only work well until a certain point and then give out completely.

Because it offers greater immunity to interfering signals, FH is often the preferred choice for co-located systems. Since direct sequence signals are very wide, they tend to offer few non-overlapping channels, whereas multiple hoppers may interleave with less interference. Frequency-hopping does carry some disadvantage in that as the transmitter cycles through the hopping pattern it is nearly certain to visit a few blocked channels where no data can be sent. To ensure seamless operation throughout these outages, a hopping radio must be capable of buffering its data until a clear channel can be found as WaveBolt does. In summary, frequency-hopping systems generally feature greater coverage and channel utilization than comparable direct sequence systems.

The WaveBolt system features numerous hopsets (also called hopping patterns) including hopsets specifically designed to avoid one or more direct-sequence channels such as those used by 802.11b radios. This reduces potential interference and allows for easier co-location with 802.11b products.

Channels, a blank means that WaveBolt avoids that channel

Hopset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
0	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
1																	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
2	x	x	x	x	x																	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
3	x	x	x	x	x	x	x	x	x	x																	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
4	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x																	x	x	x	x	x	x	x	x	x	x	x
5	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x																	x	x	x	x	x	x
6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x																	x
7	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x																	x
8												x	x	x	x	x	x	x	x	x	x	x	x	x	x	x																	
9																													x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x																												
11																	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x												

Low Power Operation for Europe and Elsewhere

The Wavebolt system complies with all European regulations for a frequency hopping system. However, it may be necessary to make a few adjustments to the radio's settings. For starters, the output power must be changed to +8 dBm (6.4 mW) from the factory default +18 dBm (64 mW). You must also choose an appropriate hopset for the particular country in which you will be operating. For most of Europe, the default WaveBolt hopset will be appropriate. Please refer to your country's particular rules for wireless devices and to the *WaveBolt AP/Radio Commands* section of the WaveBolt manual for more information.

In Europe, with the radio power set to +8 dBm (6.4 mW), the maximum gain antenna that can be used with the access point radio is 12 dBi.

It is also necessary to change a setting in the subscriber unit. The hopset will automatically be passed down to the subscriber units. However, it is still necessary to change the output power setting on each subscriber unit manually.

Radio Synchronization

WaveBolt radios are synchronized at the access point to transmit and receive data at the same time. Because all radios are transmitting and receiving at the same time, there is less chance for interference. Direct-sequence radios cannot be synchronized. They must simply avoid using the same channels

System Data Rate

WaveBolt radios transmit data with an over the air data rate of 1.23 Megabits per second (Mbps) full-duplex. Because the radio is about 7/8 efficient, this results in a true data rate of about 1.08 Mbps. WaveBolt radios are adjustable so that the 1.08 Mbps can be divided between upstream and downstream. Thus WaveBolt can be adapted to the type of data that is being transmitted. For instance a system that is mostly used for web surfing would be set so that the majority of the available bandwidth is used for downstream communications. For a system that is primarily used for email, it may be more appropriate to allocate the available bandwidth equally between upstream and downstream. From the factory, WaveBolt radios are set so that the downstream data rate is 750 kilo-bits per second (Kbps) and upstream data rate is 250 Kbps.

Access Methods

WaveBolt uses a Time Division Multiple Access (TDMA) methodology for system access. This means that each subscriber unit is give a time slot in which they can send and receive data. A subscriber on a TDMA network is guaranteed to be able to transmit and receive data. Other systems, such as 802.11b, use Carrier Sense Multiple Access (CSMA) for system access. Under a CSMA scheme, the subscriber listens until the channel is clear and then transmits. This is fine if there aren't a lot of subscribers or very little data is being passed on the network. However, if there is a lot of traffic on the network, multiple radios may try to transmit at the same time which results in what is called a collision. If a collision occurs, no data is transmitted and the radios must try again. A large number of collisions can result in poor network performance. CSMA is better suited for lightly loaded networks whereas TDMA is better suited for more heavily utilized networks.

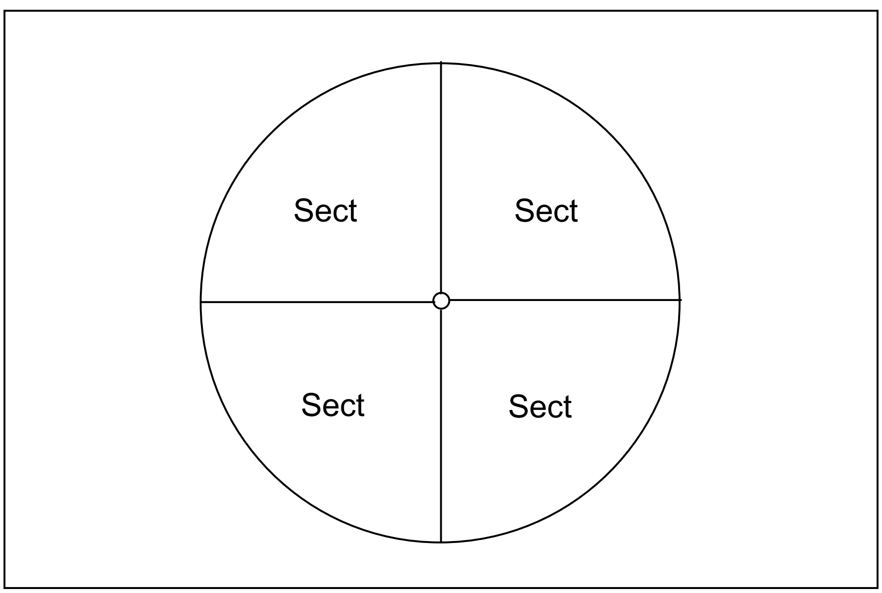
Modulation Techniques

WaveBolt uses Frequency Shift Keying (FSK) as its signal modulation and demodulation technique. In FSK, the carrier signal is modulated in frequency to create the data stream. FSK is robust and relatively insensitive to noise and multi-path. Other spread spectrum systems including 802.11b use what is called Phase Shift Keying (PSK). In PSK, the carrier signal is modulated in phase to create the data stream. PSK yields slightly better receive sensitivity than FSK.

When the modulation technique can achieve only one of two states (1 or 0), it is called binary. WaveBolt uses Binary FSK (BFSK). It is possible to achieve more than two states using the same carrier. This is called M-ary modulation. Systems such as 802.11b use both binary and M-ary modulation. While M-ary modulation results in greater data throughput, the sensitivity to noise and multi-path increase exponentially resulting in greatly reduced range. 802.11b radios will attempt to send data at the highest rate possible and then back off until an acceptable error rate is achieved. This is why users who are closer to an 802.11b access point will achieve higher data rates than those who are further away. WaveBolt on the other hand does not change modulation techniques and users will receive the same level of service no matter their distance from the access point.

Antenna Sectorization and Co-Location

The WaveBolt system is scaled to handle additional subscribers by adding additional access point radios (See the section *Expanding a WaveBolt System* for complete details). This requires that multiple radios be mounted very near each other. Because the WaveBolt system uses frequency-hopping technology, multiple radios can operate in the same area without meaningful interference as they are constantly changing the frequency on which they transmit, thereby limiting the time two radios are using the same frequency at the same time. The WaveBolt access points allow synchronization with each other to ensure that all the access point radios transmit at the same time and listen to remotes at the same time. This prevents an access point radio that is transmitting, even though on another frequency, from interfering with another access point radio that is trying to hear a subscriber radio. This is important due to the close proximity of access point radios to each other relative to the distance between subscriber radios and access point radios. This scheme allows multiple omni-directional antennas to be co-located without interference. Up to 4 Series 9 access point radios can be co-located with omni-directional antennas.



Sectorized Antenna Diagram

A common method to increase subscriber capacity is the use of directional antennas and the use of antenna sectorization. In this method, directional antennas that do not radiate in a 360° pattern are used. This allows more access point radios to be co-located since radios in different sectors cannot hear each other. For example, the CORNER249 antenna has a horizontal beamwidth of 65 degrees. This antenna allows the creation of 4 sectors.

Within each sector can be up to four Series 9 access point radios. The tradeoff with antenna sectorization is subscribers must lie in the beamwidth of the access point radio antenna to which they will connect. The figure above illustrates antenna sectorization. Although it would seem that there are gaps in the coverage, the beamwidth specified for antennas is the –3dB or half-power beamwidth – the point where the signal is 3dB below the peak power. This does not mean that there is no signal beyond 65°, only that it is reduced. Using antennas with horizontal beamwidths that are less than the desired sector of coverage is commonplace as it reduces interference between adjacent sectors. Thus 4 65° antennas will give good coverage for a 360° area.

Flow of Data

A WaveBolt Ethernet CPE uses the TCP/IP drivers in the PC or router to send and receive data. This connection is active whenever the PC or router is powered and a valid Ethernet link is present. There is no need to activate the connection. The WaveBolt USB and RS-232 systems use the Dial-Up Networking routines in Microsoft Windows® to establish a connection with the access point.

When a WaveBolt subscriber turns on their system and connects to the ISP, the subscriber PC is assigned an IP address by the access point. Once the IP address has been assigned, the PC can send and receive data over the Internet. This creates a Point-to-Point Protocol (PPP) session between the subscriber's PC and the access point. (Although it is called Point-to-Point Protocol, PPP can be used in point-to-multipoint systems like WaveBolt.) This process relies on the access point to properly format and route requests for data from the subscriber for transmission on an IP network. The access point is also responsible for taking IP-formatted traffic and formatting the data so the PC can properly interpret it.

When a subscriber wants to visit a website, a Universal Resource Locator (URL) is entered into the web browser. This request for data from the website is not sent directly to the website, but is first sent through the access point to a Directory Name Services (DNS) server. On the Internet, only IP addresses, such as 192.168.0.1 are understood. However people have a hard time remembering esoteric numbers. So the DNS server takes the URL text name and converts it to information the IP network can understand. The request for information is then sent to the Internet with addressing and routing information the IP network can understand. The service provider router acts as a "gateway" for data from the access point to reach the Internet. The router, using NAT, will attach one of its public IP addresses to the request for data to indicate where the requested data should be sent. In reality, the service provider router sends the data request to another router at the Internet wholesaler's location which in turn sends it to another router further along the Internet. The request for data will pass through many such routers before the request reaches the web site server.

When the web site server receives the request for data, it will queue the request for processing. A web server can only process one request for data at a time. When multiple requests are received by the web server, they are processed one at a time in the order they were received. So the more requests a web server receives, the longer it takes to process. When the web server processes the request for data, it retrieves the requested information and transmits it back to the requesting device. The web server will address it to the public IP address that the router used in sending the request. It may or may not take the exact same route the original request for data followed depending on how busy the network is. When the requested data reaches the service provider's router, NAT is used to translate the public IP address the router attached to the request for data to the private IP address assigned to the subscriber.

This data with the private IP address is sent to the access point. The access point knows which subscriber has been assigned that private IP address. The access point identifies subscribers by the unique factory serial number in the radio in the RF modem. The access point formats the data so the PC can interpret it and sends it to the correct subscriber over the radios. The web browser on the subscriber PC receives the data from the USB port of the PC and displays the data on the PC screen.

Security

Today's computer networks store and pass large amounts of sensitive information including credit card numbers, social security numbers and sensitive financial data. Because of the increasing reliance on computer networks for the processing of this sensitive information, security has become a hot topic among administrators and gurus within the industry.

The WaveBolt system contains security features that make it arguably more secure than even a wired network. WaveBolt features two levels of security as both the radio and the access point contain security features.

As was discussed before, the WaveBolt radio utilizes frequency hopping spread spectrum technology. The radio hops from one channel to another in a pseudo-random hopping pattern and spends only a short amount of time on any one channel. This makes it very difficult for a snooping device to lock onto the signal. The hopping pattern is known only to the access point and the subscriber unit. In addition to the inherent security of frequency hopping, WaveBolt radios also feature built in over the air scrambling of data at the bit level. The data is multiplied by a pseudo-noise code known only to the access point radio and the subscriber unit. The PPP data that is sent over the air by the access point radio and subscriber unit is encoded using an encryption key. The PPP header must be decoded using the same key at the receiving end. Anyone who does not possess the key cannot decode the PPP header and extract the data. Finally, WaveBolt subscriber units cannot communicate directly with each other. They may only communicate with an access point. They may even be assigned to a specific access point if so desired.

The WaveBolt access point also has a level of security built into it as well. Only specific IP addresses may access the system through telnet or FTP sessions. In addition, these telnet and FTP sessions as well as console port sessions may be password protected. Subscriber units require a username and password in order to be able to log into the system and to be able to pass data. Users on the system can be restricted from communicating with each other at the discretion of the administrator.

One important security feature to mention is that WaveBolt utilizes proprietary technology and therefore, only Cirronet radios may communicate with each other. This along with frequency hopping is a level of security not found in 802.11b devices.

Setting Up a WaveBolt System

Basic System

The following items are needed to set up an expandable WaveBolt Access Point capable of supporting 60 concurrently logged on subscribers:

WBAPCC	Access point card cage with power supply card, hub card and one access point card
WBAPR2/9	Access point radio assembly including mounting bracket and 24” RF cable
CBLAPxxx	Access point radio cable assembly where xxx represents the required length in 100-foot increments from 100 to 500 feet.
Antenna	One of several approved by the FCC and offered for sale by Cirronet
Power Supply	+/-48VDC power supply capable of 150 Watts power

If the system will not be expanded beyond 60 simultaneously active subscribers at a PoP, the following items are needed:

WBAPSA	Stand alone access point unit including wall mount power supply
WBAPR2/9	Access point radio assembly including mounting bracket and 24” RF cable
CBLAPxxx	Access point radio cable assembly where xxx represents the required length in 100-foot increments from 100 to 500 feet.
Antenna	One of several approved by the FCC and offered for sale by Cirronet

The antenna is determined by the desired coverage area. For example, if a 360- degree coverage area around the access point location is desired, the OMNI249 9dBi omni-directional antenna should be used. Alternatively, the CORNER249 9dBi corner reflector antenna can be used when a 90-degree sector is all the coverage that is needed. The coverage area is determined by the location of the subscribers relative to the access point location.

The above list assumes the access point is located at the service provider location where connection of the access point to the service provider network will be directly wired using a CAT5 Ethernet cable. If the access point is located away from the service provider network location, some means of "backhauling" the access point connection to the service provider location must be employed. There are two common approaches. The first is a T1/E1 connection between the service provider location and the access point location. The second is a wireless link between the service provider location and the access point location.

When using a wired T1/E1 connection between the service provider location and the access point location, Ethernet to T1/E1 bridges must be used. One bridge is used at the service provider location to connect the service provider Ethernet network to the T1/E1 connection. A second Ethernet to T1/E1 bridge must be used at the access point location to connect the Ethernet connection of the access point to the T1/E1 connection at that end. (A direct T1/E1 connection to the WaveBolt access point will be available in 2003.)

When using a wireless backhaul solution, the key requirement is that a 10/100BaseT connection is available at the access point location. Cirronet offers the WBAPBR bridge that provides a 1.23Mbps wireless link. The WBAPBR occupies a slot in the WaveBolt access point card cage and has the radio mounted near the antenna similar to the WaveBolt access point radio. In the case of the stand alone access point, Cirronet offers the WBAPBRSA stand alone wireless bridge to achieve the bridging function. Because the backhaul point to point an point to multi-point links are both in the 2.4 GHz bands, careful planning is required for non-interfering deployment.

The main determination that must be made for any backhaul solution is the required bandwidth. Each WaveBolt access point radio provides 1.23Mbps of over the air bandwidth and about 1.08 Mbps of actual throughput. Simple math indicates that about 1+ Mbps of backhaul capacity is required for each WaveBolt access point radio. This will provide for peak capacity. In browsing the Internet, it is rare that all of the capacity is used at the same time. This is due to the very nature of surfing the web where a user downloads a page and then spends some amount of time reading the information before downloading more information. An active user typically downloads somewhere between 5% and 6% of the time. Often this means that less backhaul capacity can be used without significantly impacting performance. ISPs that have dial-up users that share T1/E1 lines already have information on how to size backhaul capacity to user performance. For example, Cirronet is aware of ISPs that can offer 256Kbps download speeds to 200 users over a single T1 connection.

Expanding an Existing System

As mentioned above, the basic WaveBolt access point installation can support 60 simultaneously active users. If the service is being marketed as "always on," then the system must be sized to allow every subscriber to be logged on at the same time. If the service is not marketed as always on, then oversubscription is possible where only a percentage of the total subscriber base can be logged on at the same time. In such a case, a total subscriber population of 120 might be served with a basic access point installation where a maximum of 60 subscribers could be logged on at any one time. This would constitute a 2:1 oversubscription rate.

Whether an always on or oversubscribed scenario is used, expansion of a WaveBolt system is a straightforward and cost-effective process. Capacity for an additional 60 simultaneously on subscribers is added to a 60-subscriber card system by adding another WBAPR access point radio, another CBLAPxxx cable, and another antenna. To expand past 4 WBAPRs, another WBAPCD access point card will be needed. The table below shows the total amount of access point equipment needed based on the number of simultaneously active subscribers. To determine the equipment to be ordered to expand, find the range of subscribers that includes the desired number and subtract the amount of equipment currently installed from the equipment needed for the new subscriber number. For example, to support 200 subscribers, 1 WBAPCC, 4 WBAPRs, 1 WBAPCD, 4 CBLAPxxxs and 4 antennas are needed. To expand the system to support 300 simultaneously active subscribers, 1 additional WBAPR, 1 additional WBAPCD, 1 additional CBLAPxxx and 1 additional antenna are needed.

Subscribers	WBAPCC	WBAPR	WBAPCD	CBLAPxxx	Antennas
1 – 60	1	1	1	1	1
61 – 120	1	2	1	2	2
121 – 180	1	3	1	3	3
181 – 240	1	4	1	4	4
241 – 300	1	5	2	5	5
301 – 360	1	6	2	6	6
361 – 420	1	7	2	7	7
421 – 480	1	8	2	8	8
481 – 540	1	9	3	9	9
541 – 600	1	10	3	10	10
601 – 660	1	11	3	11	11
661 – 720	1	12	3	12	12
721 – 780	1	13	4	13	13
781 – 840	1	14	4	14	14
841 – 900	1	15	4	15	15
901 – 960	1	16	4	16	16
961 – 1020	1	17	5	17	17
1021 – 1080	1	18	5	18	18
1081 – 1140	1	19	5	18	18
1141 – 1200	1	20	5	20	20

Total Equipment Required by Simultaneously Active Subscriber Base

Installing the Subscriber Equipment

The WaveBolt Subscriber Equipment includes the following items:

1 WaveBolt™ radio modem with built-in antenna and 50-foot cable

1 Interface adapter box, either USB, RS-232 or Ethernet

1 Wall-mount 100/240VAC 50/60Hz power supply

2 Mounting clamps

1 USB or Ethernet cable

Initialization software and drivers

The radio modem is typically installed on a rooftop or outside a window where line-of-sight is available with the access point antenna. Subscribers within 1 mile of the access point antenna generally do not need line-of-sight with the antenna. A common installation will have the radio modem mounted to a pipe on a rooftop using the mounting clamps provided. Since the built-in antenna has a 90-degree beamwidth (¼ of a circle), the radio modem needs only to be aimed in the general direction of the access point antenna.

The 50-foot (15 meter) cable attached to the radio modem is routed from the outdoor radio modem location to an indoor location near the subscriber's PC. The adapter box is connected to the radio modem cable. The power supply is connected to the adapter box and provides power to the adapter box as well as the radio modem. There is no On/Off switch on the adapter box. The other end of the adapter box is connected to the subscriber's PC (or network) using the provided USB cable or Ethernet cable depending on the subscriber unit type. Note that the radio modem is the same for both the USB and Ethernet adapter boxes.

The USB and RS-232 subscriber units are added to Windows using the Windows-based "Add Modem" routines. The Ethernet subscriber unit requires no driver installation provided the standard TCP/IP drivers have previously been installed. A short initialization program is run to configure the subscriber unit before the first use.

A connection is established with the USB and RS-232 versions using Windows® Dial-Up Networking routines, similar to a wired telephone connection. The subscriber is prompted for the username and password that has been assigned by the service provider. The connection will remain open until either the PC or adapter box is powered down or the ISP terminates the connection.

With the Ethernet version, a connection is made as long as the adapter box and either the subscriber PC or router is powered. There is no need to enter a username or password when powering the system on. The username and password are stored in the Ethernet adapter during the initialization before the first use.