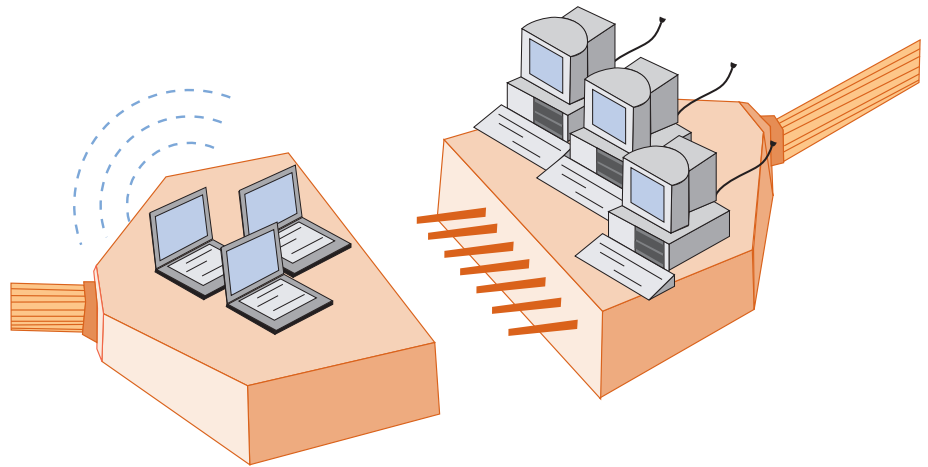


A BETTER APPROACH TO HOME NETWORKS

Wired and Wireless

pakedgedevice&software creates innovative networking products for people who demand performance, features and reliability. Our products use the most advanced wireless and networking technology and are designed for professionals to install and consumers to enjoy. You'll find our products are easy to use, productive, enjoyable and aesthetically pleasing.



1.0 Introduction

In the past decade, wireless has grown from an obscure and expensive curiosity into a practical and necessary networking technology for the home. Today's most common wireless standard is 802.11b Ethernet, also called Wi-Fi (Wireless Fidelity). The 802.11b standard is fast enough to be practical and affordable for both business and home networks. Recently, we have seen strong penetration of the next generation of wireless standard, 802.11g, which is backward compatible with 802.11b. The components can be purchased to set up a wireless network in nearly any store that sells computers, however, there are many differences among the products and how effective and reliable they are.

The appeal of wireless for the home is twofold— 1) no messy cables and 2) portability. The computers can be moved anywhere and still be connected to the network. Wireless is especially suitable for use with laptop or notebook computers, or portable devices such as PDA's, Ethernet based Remotes and Home Controls. Wireless offers users great freedom of movement and placement. However, enthusiasm for this new technology sometimes leads to forgoing the installation of a wired network, which

is just as valuable and necessary for a home.

Wired and wireless networks each have different strengths—wired networks are faster and more secure; wireless is versatile and doesn't require a cable run for each port. The ideal network includes both wireless and wired network segments combined into a single, integrated network. An integrated network enables the flexibility of a wireless network while still retaining the higher security and throughput of a wired network for confidential data and higher bandwidth applications (such as video and file backup).

It is important for anyone installing home networks to recognize wireless shortcomings that make it ill suited for a single solution for the home. In this paper we will show you why both wired and wireless networks are required for the home. Here we examine current wireless networking technology and how to use it appropriately. We will also explain the basics of how a wireless network is designed and how it can be integrated with a traditional wired network. Finally, we will show why a lot of today's networking hardware sold for the home is lacking and

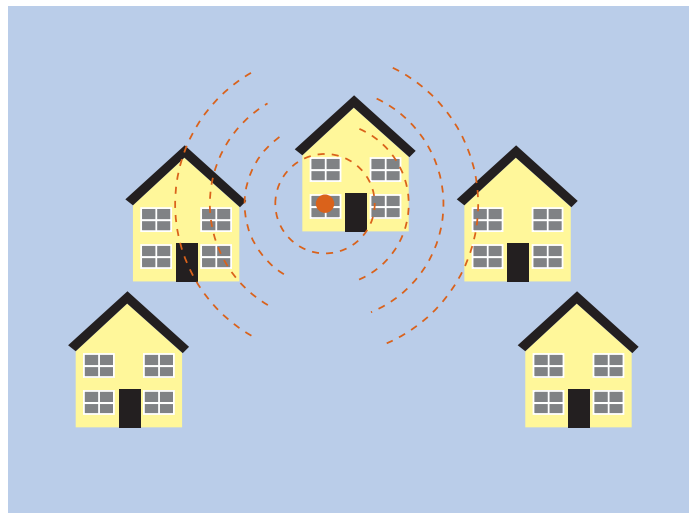


compromised in terms of security, stability, and scalability. The bottom-line - home networks deserve to be treated as indispensable and critical for a well functioning home, especially as more devices beyond computers come to rely on them.

2.0 Wireless Networks

First, it is important to be familiar with wireless and know its strengths and weaknesses. One big advantage of wireless networking is flexibility. Because there are no wires connecting network components, a wireless network gives the freedom to move computers and devices to wherever they are wanted and still be connected to the network. In addition, a wireless network can be easier to install than a wired network in a home already constructed because it does not require running many cables, concealing the cable runs, and installing wall outlets for each location.

The disadvantages of wireless are less obvious. Today's wireless networks come with an inherent set of problems ranging from serious security gaps to spotty coverage and annoying interference from other devices; these problems are especially true if the network equipment is not a)



confidential data like credit card numbers, financial data, or anything you prefer to keep private. If you don't want your personal business known, don't risk broadcasting it over your wireless network especially if the signal extends to public areas and cannot be properly secured.

2.1 Security

A primary concern when installing wireless is security. The rapid growth and popularity of wireless networks in both the commercial and residential market has led to the use of wireless for many diverse applications, including the transmission of private information. The need for privacy was the impetus to develop wireless security protocols and continues to spur efforts to make wireless a more secure technology.

The current 802.11b/g Ethernet standard includes a security protocol called Wired Equivalent Privacy (WEP), which encrypts data packets well enough to keep out most eavesdroppers. WEP encrypts each 802.11 packet separately with an RSA RC4 cipher stream generated by a 64 or 128-bit RC4 key. But several crypto-analysts have identified weaknesses in the RC4's key scheduling algorithm that make the network vulnerable to hackers. Software tools such as AirSnort and WEPcrack have already been developed to enable hackers to crack WEP and gain access to wireless networks. These software

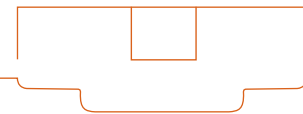
*The components can be purchased to set up a wireless network in nearly any store that sells computers, however, there are **many differences among the products** and how effective and reliable they are.*

selected properly, b) placed in the right locations, and c) configured correctly. Fortunately, these limitations can be overcome if they are considered when deciding how to implement a wireless network and what it will be used for.

For example, a wireless network will excel where freedom from a particular location is needed, it's impossible to aesthetically run a data cable, or the application does not require large file transfers. Some areas in which to use caution are applications where the network holds very

tools are widely available on the Internet. In fact, the author of this paper has cracked WEP secured networks in a little as 15 minutes.

Making WEP's encryption system 100% secure is the goal of the 802.11 working group, which began redesigning WEP in August 2001 when it became clear that its underlying cryptography, RC4 algorithm, was unsound. Such efforts should improve the security of wireless networks in the future, however, the work is far from



complete. As an interim solution to a pending 802.11i standard, a consortium called the Wi-Fi Alliance has created a subset security protocol called Wi-Fi Protected Access or WPA that offers code breaker-hostile features like Temporal Key Integrity Protocol (TKIP). Using TKIP, up to 500 trillion possible keys can be used with a given data packet, making brute-force cracking virtually impossible.

2.2 Speed and reliability

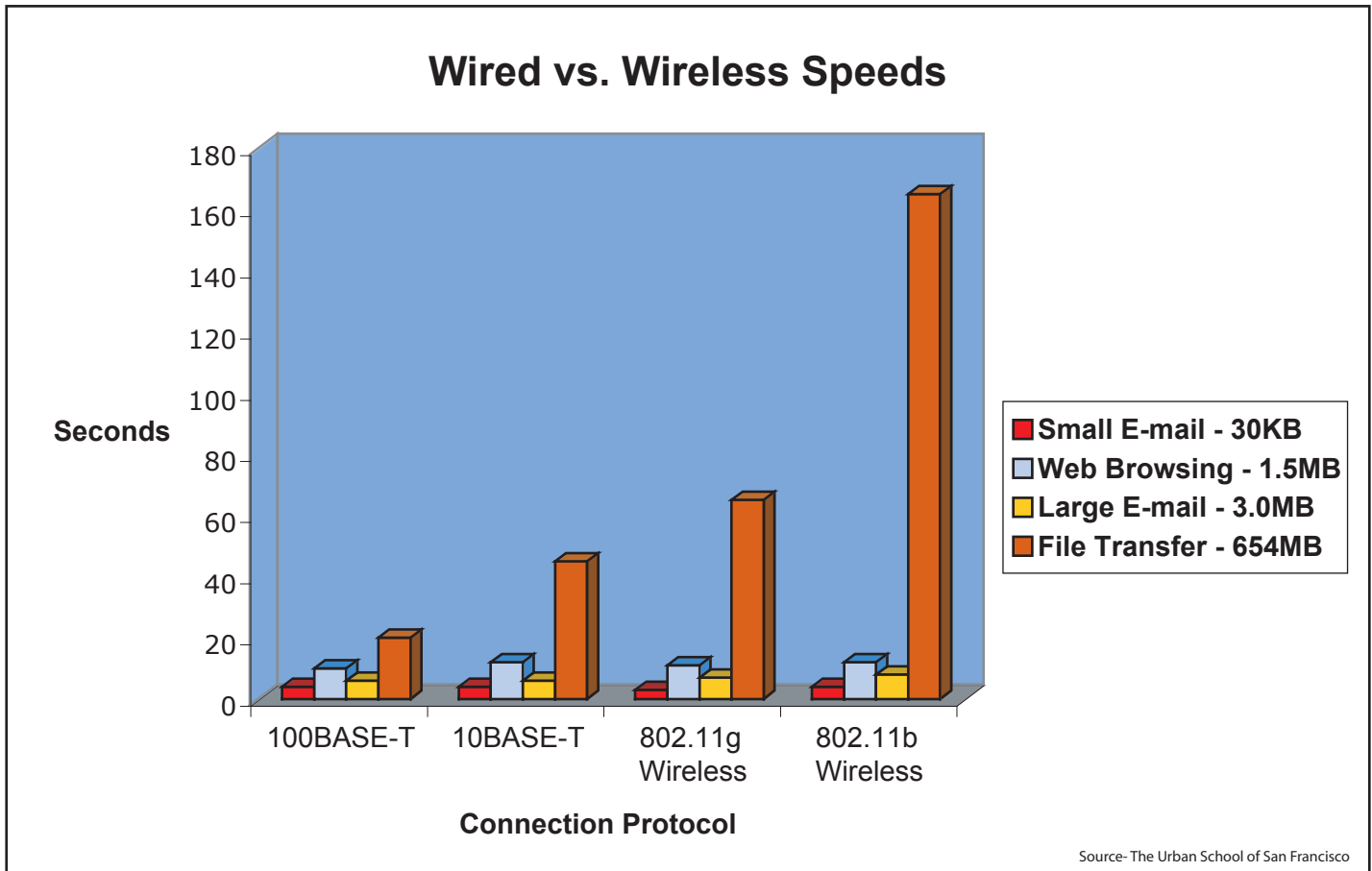
As wireless security methods are strengthened, a trustworthy and often overlooked method is to reduce a wireless signal so it does not exceed property lines. After all, it is impossible to hack a wireless network where no signal is present. A wireless access point should not be placed where the signal will greatly exceed its intended area of use. Because it is difficult to move wireless access points once they are installed, the optimal solution is a wireless access point for which the installer can reduce power output if the signal exceeds its area of use.

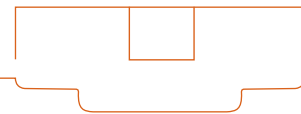
802.11b and 802.11g claim speeds of 11 Mbps and 54 Mbps, respectively. A more realistic estimate of actual throughput is about 3.5 to 4.5 Mbps for 802.11b and 15 to 25 Mbps with 802.11g. Speeds are even further reduced if WEP or WPA is enabled. For example, WEP can slow

a wireless network by 20 to 50%. Another key point to remember is speeds are reduced further as the signal to noise ratio is decreased, meaning that speeds could be dramatically further reduced as the user moves further away from the access point, if there are a lot of barriers or obstructions between the user and the access point, or if a source of interference is present (receiving a call on a 2.4 GHz phone or turning on the microwave).

It is important to keep network speed in perspective as the home network is designed. Throughput in the 3 to 5 Mbps range is still much faster than broadband Internet access; it is fast enough for using the internet. But, it is often inadequate for larger applications where large files are stored centrally and constantly exchanged from one device to another. Some examples are Quicken, PowerPoint, Video Editing, DVD Movie Servers and uncompressed music files.

When designing a network, take a realistic look at the bandwidth requirements and add wires where applications need to transfer large files regularly, or lightning-fast network response is needed. For all others, strategically placing wireless access points close to the point of use should be adequate to serve current and future unplanned requirements.





2.3 Environmental concerns

As stated in the last section, the environment can affect wireless network speed and reliability, and a wireless network may affect electronic devices within the environment. Therefore, take a good look at the space where you intend to install your wireless network.

2.3.1 When your house gets in the way

When you set up your wireless network, chances are you won't get the network to operate effectively at more than a fraction of the promised 300 feet, because the distance given as the network range is the maximum distance accomplished in open space under ideal conditions. Walls, furniture, appliances, and other large structural features can interfere with wireless transmission. The wireless network will compensate for some of this interference by dropping to a lower speed, but you're still likely to find that transmission distance is much shorter than anticipated.

Some building material provides special obstacles to wireless transmission. For example, the solid stone walls, brick, or heavy coats of plaster on lathe in older, historic homes can stop wireless transmission cold. For this reason, a wireless installation in an old building may require more access points than in a comparable modern building. In sum, at greater distances, it may not be practical to use the connection because of its dramatically

Wireless offers users great freedom of movement and placement. However, enthusiasm for this new technology sometimes leads to forgoing the installation of a wired network, which is just as valuable and necessary for a home.

slower speeds. A higher output power access point will extend these ranges, however, the network speeds might be too slow for applications that require high data throughputs.

2.3.2 Interference from other electronic devices

The 2.4-GHz frequency used by 802.11b/g wireless is appealing for many wireless- and electronic-device manufacturers because the government doesn't require a license to use it. But no license also means there's no entity to coordinate use in this frequency. Interference from and with other 2.4-GHz devices can be a problem with wireless networking, especially in dense urban environments, apartments, and town homes.

Common devices that can interfere with or have interference caused by wireless network include:

- Baby monitors
- Garage-door openers

- Cordless phones
- Microwave ovens
- A/V senders
- Satellite radio (i.e. XM radio)
- Energy-saving light bulbs
- Other wireless networks
- Medical devices such as diathermy machines

Many of these devices, because they share the same 2.4-GHz spectrum, can noticeably degrade the wireless network's performance. A wireless network can also interfere with the performance of other devices operating in the 2.4-GHz spectrum. With devices such as portable phones, this doesn't matter much, but in the case of critical medical devices, a nearby wireless network can be life-threatening. Another way to minimize or eliminate interference is to simply remove or reposition the devices that cause it. Keep devices such as microwave ovens at least six feet from wireless access points, better yet, place microwaves inside a kitchen cabinet and line the inside with a metal screen.

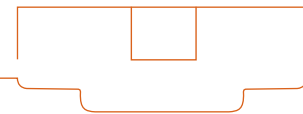
Finally, whatever brand of wireless access point is installed in the home, the device should have both the ability to shield itself as much as possible from interference and the logic to automatically adjust transmission speeds to maximize data throughput performance depending on environmental conditions. One important note is that wireless access points that constantly try to send and receive data at high transmission speeds will not

be the best performers. If environmental conditions are bad and speeds are not reduced to match, data packets will be lost and the wireless access point will have to constantly resend packets, decreasing overall data throughput

performance.

2.3.3 Compatibility

Something else to watch out for when selecting a wireless access point for your home network is compatibility. Some vendors—even though they are subject to 802.11b/g compatibility tests—will decide they have a better solution for speed or security and will build proprietary solutions into their wireless equipment. For example, these vendors will promise speeds beyond 54 Mbps of standard 802.11g products, however, not all 802.11g products are compatible with this equipment and therefore will not experience the advertised performance improvements.



3.0 Setting up both a wired and wireless network

3.1.1 What is a Router, Switch and Wireless Access Point?

In order to setup a wired and wireless network, several devices are needed. First is the DSL or Cable modem, depending on which type of broadband service is subscribed to. This device is typically provided by the broadband provider and is needed to communicate with the service provider's backend equipment. This device allows the internet data packets to travel in the same cable as either the cable TV signal or telephone voice signal, depending on whether there is a Cable or DSL broadband connection. The second required device is called a router. A router forwards data packets from one local area network (LAN), (in this case your home) to a wide area network (WAN), (in this case the broadband provider's backbone equipment). The router reads the network address in each transmitted frame and makes a decision on how to send it, using the most expedient route.

Routers are used also to balance traffic, filter traffic for

security purposes and for policy management (keeping rogue users off the network). In some instances they act as gateways that convert from one protocol to another. The third device that is necessary is a LAN switch that cross connects the many different network segments or ports to which computers, wireless access points, and/or servers might be attached. A switch is somewhat similar to a router in that it passes data packets from one destination to another; however, it works at a different data link layer, which enables it to be much faster. A switch is not to be confused with a hub. Although they might appear to do the same thing because a switch can simply replace a hub in an Ethernet network, a switch is much faster. It does not need to share bandwidth among the different ports and it has a different set of functions and procedures, which allows it to avoid collisions among data packets.

A good analogy is to picture a traffic intersection. A hub is like an intersection without a stop light at which traffic from different directions needs to manage itself to pass through the intersection. Sometime collisions do occur, slowing everything down. A switch, on the other hand, is an intersection with many temporary bridges that can pass traffic from one direction to another without

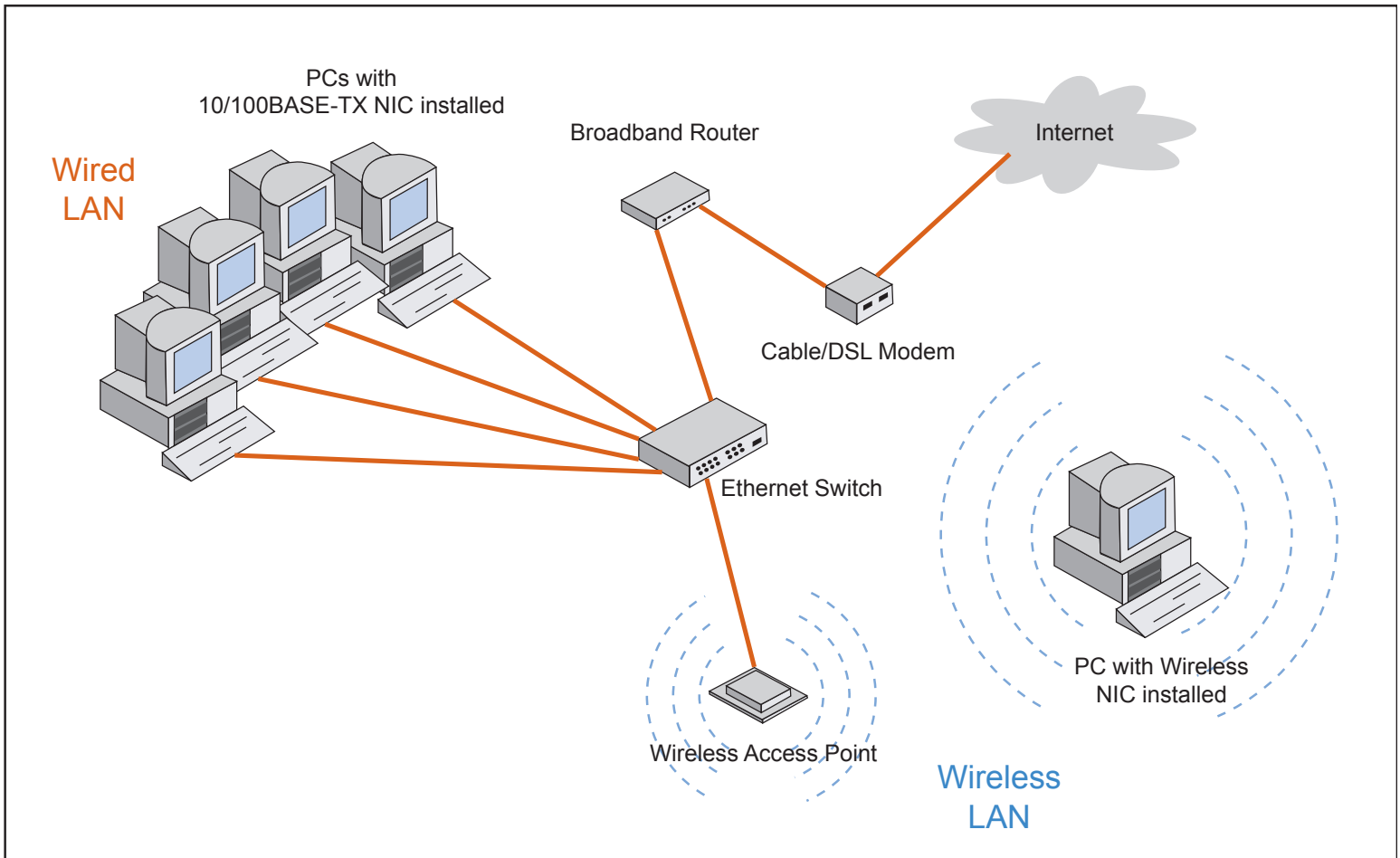


Figure 1



affecting traffic in a different direction. If someone needs to go in a different direction, a new temporary bridge is quickly erected to allow all traffic to pass simultaneously. Continuing with this analogy, a router is like a check point and informational booth. As each data packet passes, the router gives it directions, or if it looks foreign, it might ask for

into the switch, including computers, servers, printers and wireless access points.

Figure 1 describes a network in which the router, switch and wireless access point are separate, independent devices. As residential networking becomes more

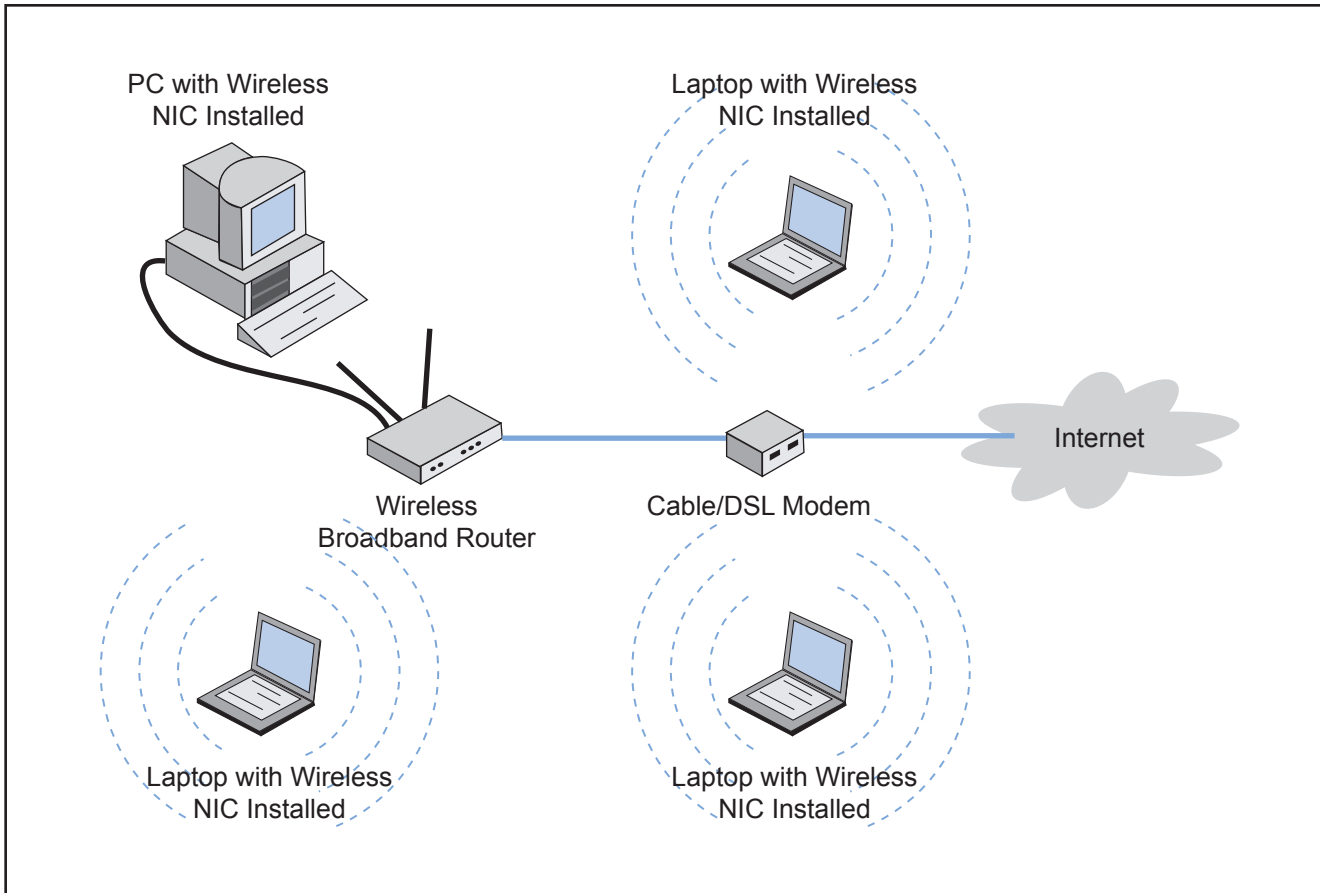


Figure 2

special credentials before the router lets the packet pass.

The final device that is required is the wireless access point, a bridge or translator between the wireless clients and the wired network. In very easy terms, the wireless access point will simplify communication with a wireless laptop in some type of standard language, in this case 802.11b/g, and then translate the data packets to a wired standard, in this case Ethernet or 802.3. Of course, most wireless access points have other functions such as security, but translating from the wireless world to the wired world is their prime purpose.

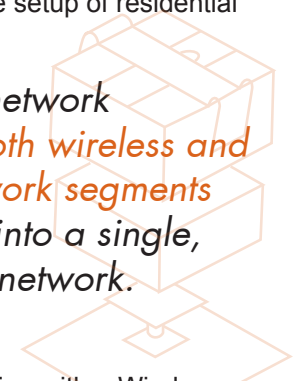
3.1.2 Putting the Pieces Together

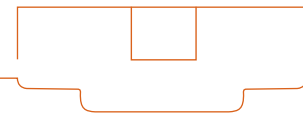
If all of the devices are taken together and connected, a network will be created as shown in Figure 1. At the point of entry is a DSL/Cable Modem. Connected to the DSL/Cable Modem, is the router, which is then connected to the switch. Finally, all the other ports in the house connect

popular, and in an effort to simplify the setup of residential networking, these three devices are combined into one device or an all-in-one solution typically called a Wireless Broadband Router.

The ideal network includes both wireless and wired network segments combined into a single, integrated network.

Figure 2 shows a network configuration with a Wireless Broadband Router. The Wireless Broadband Router replaces the router, switch, and wireless access point, and the Wireless Broadband Router is connected to the DSL/Cable Modem.





3.1.3 A Wireless Broadband Router Falls Short

Wireless Broadband Routing has simplified home networking so that more homes have networks today. In fact, the Wireless Broadband Router has been so successful that a majority of homes today use this single device rather than a separate router, switch, and wireless access point. However, the success of Wireless Broadband Routers in introducing homes to networks also created a market of products for the home that require more performance, reliability and scalability than what a Wireless Broadband Router can provide. Essentially, it has given the home owner a taste of the benefits that a home network delivers. A good analogy is the introduction of Ford's Model-T. The car gave buyers a glimpse into the convenience, speed and reliability of automobiles. However, as soon as the novelty of the Model-T wore off, buyers and new manufacturers realized that cars could be more reliable, powerful, ergonomically friendly, and aesthetically pleasing than the Model-T.

Today, most Wireless Broadband Routers are simply placed in a closet or on top of a desk wherever the

the wireless access point needs to be mounted on the ceiling.

If a Wireless Broadband Router is buried in a closet or behind furniture, the placement automatically greatly reduces the wireless performance. If the closet where the Wireless Broadband is located is not in the center of the house, it will have great difficulty achieving wireless signal on the other side of the house. In fact, your neighbor on the side where the Wireless Broadband Router is located might have better signal than you, thus opening up potential security problems. Also if the closet is located on the first floor of a second story house, wireless signal will most likely be very weak on the second story, especially directly above the closet location due to the Wireless Broadband Router antenna's natural emitting pattern.

The concept of having a separate router, switch and wireless access point to achieve the best network for the home is not new. Almost every corporate and public network is designed and implemented in this fashion. It is impossible to design an all-in-one device with the right routing, switching and wireless access point capabilities

*A lot of today's networking hardware sold for the home is **lacking and compromised** in terms of security, stability, and scalability.*

broadband connection enters the home. With this type of installation location, it is difficult to achieve strong coverage, scalability, and pleasing aesthetics. In any installation, the router should be placed close to the DSL/Cable Modem and hidden from everyday view because of the many wires which connect to it. This will typically mean the router will be in a closet or enclosure at the Broadband point of entry into the home. The switch, as well, should be in a closet, hidden from everyday view; however it needs to be where the "Home Run" terminations are all located, leading to an overwhelming amount of cables.

A dedicated closet or other enclosure is the best place for the router and switch. Most would agree that exposed cable bundles are not aesthetically pleasing, but more importantly, a closet or enclosure will provide protection from tampering and accidental impact, which can disconnect fragile cable connections and in turn cause trouble for the network.

With the router and switch in the closet, what does this mean for the wireless access point? The wireless access point needs to be in the highest locations and not obstructed by radio signal attenuating material to achieve the strongest coverage and therefore good data throughput performance. This very important point means

for every different home, every different need and every different user. Each home network implementation is unique and each home network deserves the flexibility, quality and performance that separate devices provide. A good example is reference quality audio and video equipment. Most reference level systems have separate components connected together to achieve the best performing system. You can always find a separate tuner, pre-amplifier and multiple amplifiers to drive speakers, but each component must be selected carefully to support what the user wants to accomplish.

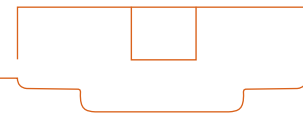
3.1.4 A Reference Quality Residential Network

Creating a reference quality network requires separates as well: a router, switch, and multiple access points to support the size of coverage area.

3.1.3.1 Router

First of all, a network will need a router. There is a vast selection with different features and performance levels on the market today. Once the capabilities of the different routers have been investigated, you will see what limited options a Wireless Broadband Router has.

There are some basic capabilities that a broadband router has to have to network with the broadband internet provider, such as static, dynamic or PPPoE, and basic



networking protocol support such as DHCP (issuing IP addresses to the users) and NAT (translating IP addresses between internal and external networks) to create the basic network. All routers will have these basic capabilities.

As for other router options, it will depend on what the home owner wants to accomplish with the network now and in the future. It is not feasible to cover all the options on the market today; however, some of the more essential ones for a resident are as follows: First, the router should be mountable, preferably in a rack and in a secure location. This is a basic requirement. A router needs to be protected from accidental impact and tampering. It may be surprising to know how many networks we've fixed where the problem was due to a child unplugging a cable or a cleaning person accidentally pushing a button which turned off a portion of the network. Along the same line,

As wireless security methods are strengthened, a trustworthy and often overlooked method is to reduce a wireless signal so it does not exceed property lines...the optimal solution is a wireless access point for which the installer can reduce power output if the signal exceeds its area of use.

the router should have a rugged metal housing and high quality electronics.

Most of the time, home owners take these things for granted and typically don't want to pay extra for these types of units. However, for the extra investment now, the potential downtime aggravation will be greatly reduced in the long run. Higher price point routers generally have faster processors and more memory, which is very

important in various firewall activities such as Stateful Packet Inspection (SPI) - the faster packets are inspected, the faster they will be distributed.

This leads us to another key feature that a router should have: the latest in firewall functionality to prevent various attacks from the internet. Also, VPN capabilities are becoming more important as more people want to connect securely to work from home, access files securely on a home computer on the road, or even control their vacation home's numerous functions securely with widely available IP network based products such as web cameras. On the other hand, a lot of home owners with children want to control when and how long their kids are accessing the internet, which websites are allowed, and which they want blocked. There are many routers with various content blocking and filtering capabilities, including one which can

automatically send real-time email alerts and reports.

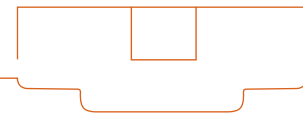
3.1.3.2 Switch

The second component is the switch. Even more than the router, the switch should be rack mounted because many cables will terminate at the switch. Most switches are usually placed in a closet or out of everyday view because of the unsightly amount of cables. Why all the cables? Since all homes should have a wired and wireless network, every single room in the house will at least have one wired port. These wired ports will be connected to the switch. In addition, in the home office or behind audio/video equipment, it could take as many as six ports to connect the computers, printers, fax line, home phone line and office phone line.

It should be fairly obvious why Wireless Broadband Routers, which typically come with only 4 ports for a wired network, are inadequate for a majority of homes. The average 3,000 square foot home should have 24 wire ports available for computers, printers, wireless access points and other Ethernet devices. Another key feature a switch should have is management capabilities, or a Managed Switch. A managed switch is no more complicated than an unmanaged switch to install, and when you don't configure the management portion, it's plug-n-play. However a managed switch can be configured to provide extra security for wireless networks, and it can be reconfigured to meet specific future network traffic needs.

A managed switch is particularly important when the wired network contains data the home owner wants to keep private. A managed switch can keep general network traffic off the wireless segment and vice versa. Essentially, a managed switch allows installers to virtually segment the network by using software without physically rearranging the devices or network connections. This segmentation makes the network more secure because each network segment keeps the traffic to itself. It also makes sure the wireless access points transmit only data going to wireless computers—data traveling on the wired network segment is not transmitted over the wireless network segment.

The installer can take network segmentation to new creative levels, depending on the home owner's requirements. For example, children's computers can be on a different network if parents don't want the kids to have access to certain household devices. Another key feature of managed switches is traffic prioritization. With the high adoption of Voice-Over-IP, or placing telephone calls over the household internet connection, voice traffic needs to be prioritized over data traffic. If priority is not given to voice traffic, voice conversations will sound like a bad cellular connection, if someone is moving large media files on the network, e.g. downloading a video file on the internet.



3.1.3.3 Wireless Access Point

The last component is the wireless access point. Similar to a quality audio system where the number of amplifiers added depends on the number of speakers and the amount of space the sound needs to fill, the number of wireless access points should be installed based on the desired coverage area. The current general complaint among home owners with wireless networks is the lack of coverage in key areas of their homes, and because of the commercial success of Wireless Broadband Routers (a single device), the general approach is to try to make a single wireless access point cover a larger area. Unfortunately, this approach is hindered by constraints which do not allow for improvements to the point at which most home owners would be satisfied. The simplest and surest approach is to add more wireless access points to ensure complete coverage. After all, data throughput and, therefore, satisfaction is directly related to proximity and the number of obstacles to the wireless access point.

The optimal place to install a wireless access point in most homes is embedded in the ceiling. The ceiling location is high and if the finishing aesthetics of the wireless access point are discrete and attractive, the wireless access points can be placed at the optimal locations for performance, rather than in good hiding places for electronic devices. Beyond the form factor, there are many other aspects of a wireless access points that will ensure satisfaction. Look for a solid metal housing and quality components. The better wireless access points will even have heat sinks on key semiconductor components to improve long term reliability.

Also, a wireless access point with a variable high output power rating is an important feature (the maximum allowed by the FCC is 200 mW). The higher output power rating is not so much for broadening coverage as it is for providing reduced quality coverage and security. Just like a stereo amplifier, if you push the amplifier to its limits, undesirable characteristics appear, such as distortion. The variable power aspect of the wireless access point allows the installer to reduce power to the intended area of coverage, i.e., within the inside of a house. After all, if no signal is present outside a house, or even worse on public sidewalks or streets, there is virtually no chance that the wireless network will be penetrated by unauthorized users.

4 Installing a Wireless Network

4.1 First a Brief History of Wireless

4.1.1 802.11—the first wireless Ethernet

The precursor to 802.11b, IEEE 802.11, was introduced in 1997. It was a start, but the standard had serious flaws. 802.11 supported speeds of only up to 2 Mbps. It

supported two entirely different methods of encoding—Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS)—leading to confusion and incompatibility between pieces of equipment. It also had problems dealing with collisions and with signals reflected back from surfaces, such as walls. These defects were soon addressed, and in 1999, the IEEE 802.11b Ethernet standard arrived.

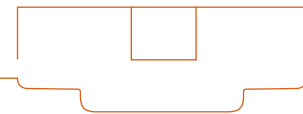
4.1.2 802.11b and g—wireless Ethernet refined

The 802.11b extension of the original 802.11 standard boosts wireless throughput from 2 Mbps all the way up to 11 Mbps. 802.11b can transmit up to 200 feet (61 m) under good conditions, although this distance may be reduced by the presence of obstacles, such as walls.

The 802.11b upgrade dropped FHSS in favor of DSSS. DSSS has proven to be more reliable than FHSS, and settling on one method of encoding eliminates the problem of having a single standard that includes two kinds of equipment that aren't compatible with each other. 802.11b devices are compatible with older 802.11 DSSS devices, but they're not compatible with 802.11 FHSS devices. Also 802.11b differs from standard 802.3 and 802.5 wired Ethernet only at OSI Layers 1 and 2; it's interoperable with standard wired Ethernet. Because it's a real Ethernet standard and looks like Ethernet to the applications, 802.11b is perfectly compatible with both Microsoft® Windows® and Macintosh® OS, as well as more unusual operating systems such as Linux®. 802.11b is the most widely available wireless standard today.

802.11g, on the other hand, is an extension of 802.11b and operates in the same 2.4-GHz band as 802.11b. It brings data rates up to 54 Mbps using OFDM (Orthogonal Frequency Division Multiplexing) technology. Because 802.11g is backward-compatible with 802.11b, an 802.11b device can interface directly with an 802.11g access point. The more expensive access points will support both b and g users and still maintain the higher speeds for the g users. The cheaper access points will decrease the overall speed of the network to b levels whenever there's a b client on the network even though g clients are requesting the higher speeds.

The wireless access point needs to be in the highest locations and not obstructed by radio signal attenuating material to achieve the strongest coverage and therefore data throughput performance. This very important point means the wireless access point needs to be mounted on the ceiling.



4.1.3 Up-and-coming wireless standards

4.1.3.1 802.11a

Available at the same time as 802.11g, 802.11a uses a different band than 802.11b and g—the 5.8-GHz band called U-NII (Unlicensed National Information Infrastructure) in the United States. Because the U-NII band has a higher frequency and a larger bandwidth allotment than the 2.4-GHz band, the 802.11a standard theoretically achieves speeds of up to 54 Mbps. 802.11a is having limited success because it only achieves comparable speeds to 802.11g and is not compatible with 802.11b, which is today's standard. Because of the low adoption levels, cost of this equipment is high.

4.1.3.2 802.11n

With the standard not fully defined and no anticipation of approval until the middle of 2007, some vendors are starting to release product based on their interpretation of what the standard should be. They are calling it Pre-n in an effort to convince the buyers their product might be compatible with 802.11n when it is fully defined. 802.11n is too far off at this point to say what it will be; there are two major industry working groups, each trying to push their own version of the standard.

4.2 Considerations before Installing a Wireless Network

The perfect time to plan a wireless network is before commencing a remodel, and/or new construction, when cables can be easily routed to the Wireless Access Points in the most optimal locations. Selecting the proper location(s) and number of Wireless Access Points

Home networks deserve to be treated as indispensable and critical for a well functioning home, especially as more devices beyond computers come to rely on them.

will greatly enhance wireless coverage and, therefore, enjoyment. Because radio wave behavior is so difficult to predict outside the laboratory environment, the best wireless network installations all begin with extensive planning. First, perform a site survey, creating a room layout, noting building material and obstructions, and identifying interference sources. From this information, determine Wireless Access Point locations. Next, perform a mock installation, temporarily placing Wireless Access Points in planned locations and measuring Signal Strength and/or Throughputs.

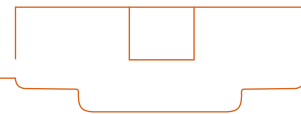
Network and power connections must also be considered. Often the best place for access points is on the ceiling. While an access point can easily be mounted on the ceiling, most homes do not have Ethernet and power connections on the ceiling. A partial solution to this problem is to run just an Ethernet connection to the access

point but to use an access point that can be powered through the Ethernet cable. These access points get power from a device in the wiring closet that provides DC power over the unused wire pairs in the UTP Ethernet cable. This feature eliminates the need to run an AC power cable to the access point, making installation easier and cheaper. Given that not every installation affords the luxury of using the approach described above, the following are some basic rules to follow when designing wireless networks that should yield good results.

- As a rule of thumb, you'll need about one Wireless Access Point for every 2,000 square feet of inside living space, depending on the type of building material used to build the home. Lathe and plaster walls, and concrete walls will require more Wireless Access Points. If walls are constructed of sheetrock, as in most new homes, fewer Wireless Access Points will be required.
- It's better to install more Wireless Access Points than fewer, as long as you have three channels of separation among Wireless Access Points. In North America, Wireless Access Points are allowed to use 11 channels; therefore, you can use four Wireless Access Points in most homes without interference issues. For installations requiring more than four Wireless Access Points, the two Wireless Access Points with the closest channels should not have overlapping radio emitting patterns.
- The advertised range of all Wireless Access Points on the market today describes ideal conditions. In reality, due to interference, walls, and other obstacles, the actual range will be much less. As a rule of thumb, to have complete overlapping

coverage, you should space Wireless Access Points 30 feet apart, assuming they each have three channels of separation.

- During signal strength tests, even though you get a signal at the edge of your wireless network, it might not be practical to use the network at that location. If the signal strength is weak, throughput speeds will be slow, greatly limiting the type of application (e.g., copying large computer files).
- Try to have strong wireless coverage at all locations in the home. The ultimate location for laptop use can change over time and new devices that need wireless networks may be installed at future dates. When in doubt, add an additional Wireless Access Point. If the signal is too strong, the Wireless Access Point power can always be reduced.



- In homes where attic space will be accessible after construction, run extra Category 5e wire to the attic (leaving enough to extend it anywhere in the attic), allowing the possibility of adding more Wireless Access Points if coverage is not sufficient.
- For every wall a Wireless Access Points signal must penetrate, expect a drop in signal strength (around 6 db for sheet rock). If your access point must penetrate an exterior wall, the signal loss will generally be greater. If the exterior wall is stucco (plywood with wire mesh and cement) don't expect a lot of signal to penetrate, as this material configuration greatly attenuates 2.4 GHz radio waves. Other home materials that 2.4 GHz radio waves will have difficulty penetrating include brick work (e.g., chimneys and walls), concrete and stone tile floors (for example, if the second story floor is all concrete, it will be hard to achieve a strong signal on the first floor), and sheet metal, such as ducting or aluminum siding.
- If there is concern about unauthorized users on the network, set up the wireless network so that it does not extend beyond the property line. Although there are security features on all Wireless Access Points, activating them generally makes the network slower and more time consuming to maintain. The best security is not to broadcast the signal outside the home's property lines. No one can hack what they can't reach!
- The biggest source of WiFi interference in homes is 2.4 GHz phones. These phones really do interfere with wireless networks, especially the frequency hopping type. It's better to upgrade to 5.8 GHz phones or go with 900 MHz older ones. Another source is microwave ovens. Expect reduced performance when these are in operation.
- Coverage and performance are best when Wireless Access Points are installed in high locations, such as second story ceilings. As with any antenna, the higher the location, the better the performance.
- Never install a Wireless Access Point "behind" an object. The best performance occurs when you have an unobstructed line of sight connection with a Wireless Access Point.
- Finally, try to place each Wireless Access Point where a Wireless Network will be used most often. Most WiFi devices are generally low powered devices that are not designed to transmit over long ranges.

and set it up and start enjoying the best video technology the market had to offer. Now, in order to enjoy the best in video entertainment, a family needs to call in professionals to help them select the best equipment. The system of devices could be comprised of up to 16 different pieces of equipment, from a plasma television to a pre-amplifier to speakers. The installation could take a few days to as much as months, and might including reinforcing a wall to hang a plasma television, making holes in walls to install speakers, and erecting custom cabinets in which to place all the equipment.

Wireless access points that constantly try to send and receive data at high transmission speeds will not be the best performers.

With all the new technology today and coming in the future that relies on an Ethernet based network, the days will soon be gone when a home owner can go to the local electronic store, purchase a

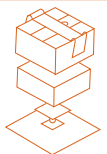
Wireless Broadband Router and set it up by himself. The home owner will need to call in a professional to help design the right network, select the right equipment and integrate them properly.

In sum, it is important to implement a wired network in addition to a wireless network for different types of applications. An all-in-one Wireless Broadband Router is ill-suited for most homes where a network needs to be reliable, high performance, and scalable. A lot of the approaches we discussed are not projects that an average home owner can design and implement. A qualified installer can help the home owner make the right selection and perform the installation and offer the required support. The result will be a world class network that will not only support all computer applications today, but also will support all applications of tomorrow, such as media servers, video on demand, IP based home controls, voice-over IP, and IP based home automation products.

5.0 Conclusion

Not too many years ago, a family could go to the local electronic store, purchase a state of the art television, load it up in the back of their station wagon, come home

pakedgedevice&software inc.
 PO BOX 1973, San Mateo, CA 94401
 Main - 877-274-6100, Fax - 650-347-5138
 sales@pakedge.com, www.pakedge.com



Company Background

Founded in 2003, Pakedge Device & Software was created to fill the voids in high performance home computer networking products. Before our company was founded, computer networking products for the home were too compromised, unreliable and lack the "right" features. Pakedge Device & Software delivers the ultimate wireless and networking products for the uncompromising home owner. Our products speak for themselves.