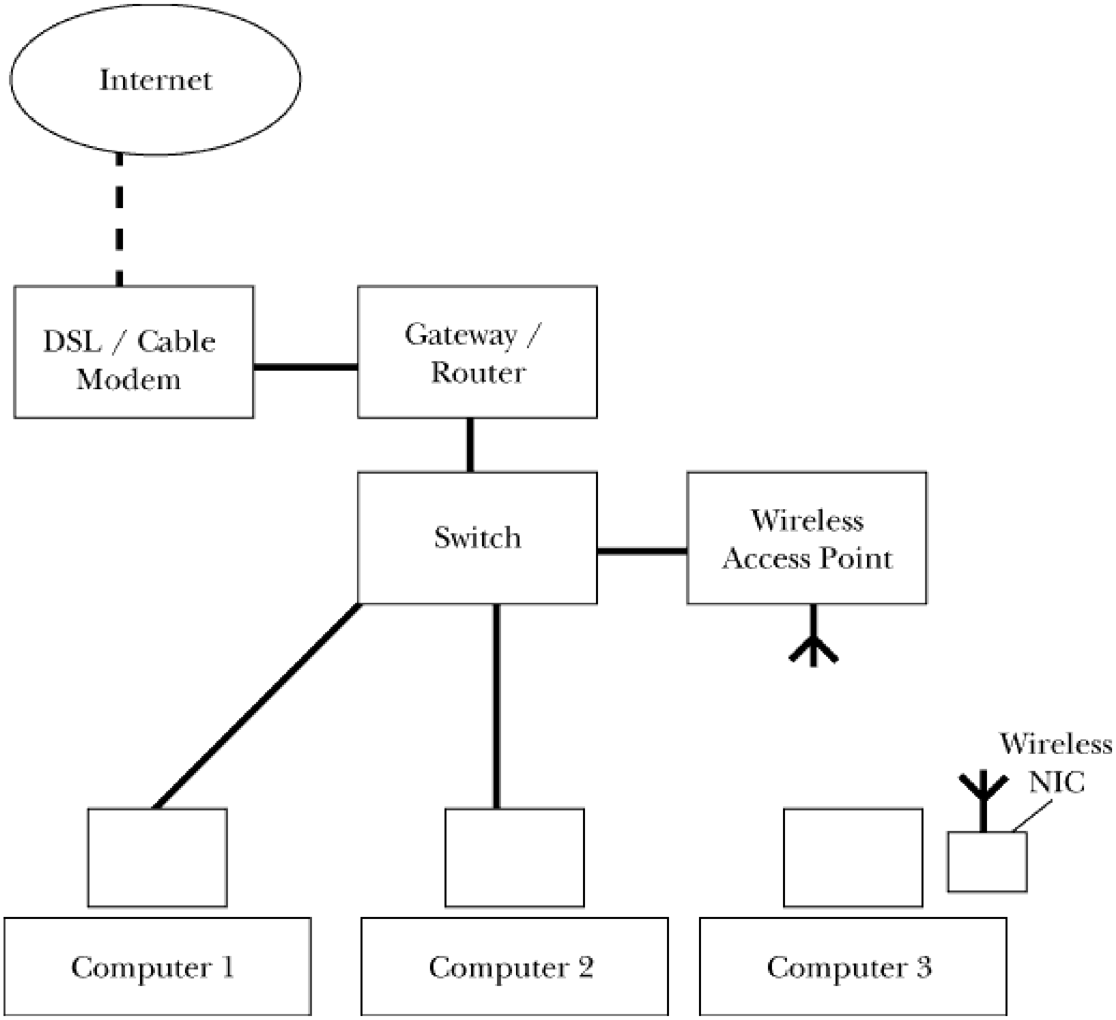
Wireless Workout

Why would a company called **Cable**Wholesale.com send out information about a technology that does not need cables? Wireless networking is a fantastic way to connect home computers, and its advantages are easily recognizable, but this technology is not for everyone. Wireless networks are slower than their copper counterparts, have serious security concerns, can interfere with or be affected by home appliances, and may not even work depending on the construction of your home.

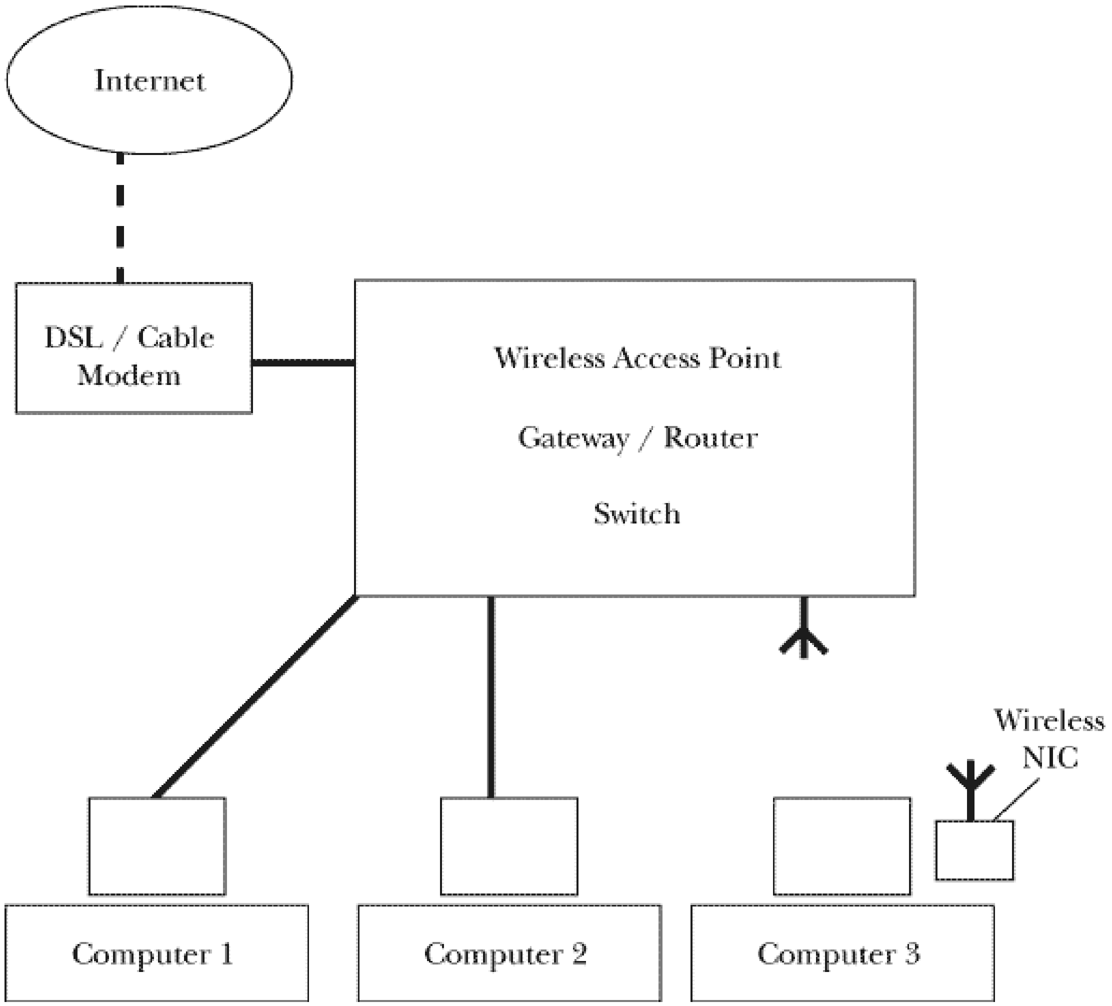
Basics

Wireless networking allows a computer or network device to be connected to other computers or network devices without wires. While this practice is in no way new, its price point, speeds, and ease of use have brought it into range for the average consumer.

A wireless network consists of several parts: a switch, a wireless access point, wireless networking cards, and some computers. As most people who have more than one computer also have broadband connections, we have included a cable / DSL modem and a router in the diagram below. (If you missed our article series on home networking, you can find both parts technical articles.)



Sometimes these devices are sold in one package. It is quite common for routers to also contain a small switch. These devices are typically marketed toward home users, while the separate components are generally geared toward enterprise use.



Security

There are a few guidelines that should be followed with any network, but due to the exposed nature of wireless networks, some of these become dangerously important.

Change the default password!

Golden Rule. Do not even think about breaking this one.

Turn off DHCP

Dynamic Host Configuration Protocol is an easy way for someone to get on your local network and initiate attacks against computers that normally protected by a firewall, or just use use your Internet connection. Not using DHCP requires a little more configuration on your computers, but this simple protection will stop a lot of the basic attacks.

Use encryption

It does not take much equipment to scan a wireless network and record all the data that passes between a host and the access point. Encrypting this data between your host and the AP makes it more difficult for this data to be used if it is intercepted.

Authentication

There are several common methods of verifying that a computer is authorized to use a wireless routers. Check the manuals for your wire access point and wireless networking cards to see which methods are supported.

Nothing is "Hacker Proof"

In order for an electronic device to be "Hacker Proof", it must be indistinguishable from a rock. If there is a wire connected to it, or electricit running through it, there's a way to hack it. If you find a nice shiny box that says "Hacker Proof" on it, put it down and find something else because they have spent more money on marketing than on research.

While some view the sharing of wireless networking as a public service similar to writing open source software, others see it as a source of litigation. If someone does something illegal while connected through your equipment, and you have taken no measures to prevent someone from using your connection, you could be considered an accessory. However, there is currently no legal precedence for who holds full responsibility for the crime, so legal speculation is just FUD until a ruling is made.

Free Surfing Lessons

While it's not technically illegal (yet), using someone else's Internet connection definitely fits the kindergarten definition of 'taking without asking'. The simplest way to attach to an open network is with a DHCP client. Just configure your wireless network card to DHCP to the IP of an available router. Often times the drivers for your wireless networking card will come with a simple network discovery tool and show you an open network you can access. More advanced versions of these tools are available for free. PrismStumbler is an open source project that will try to get as much information about local wireless access points as possible. NetStumbler is also quite popular, and is known for being easy to use. These tools even have GPS add-ons so you can drive around map the areas you had connectivity. This is called "War Driving". Once you have the required information from your stumbling utility, you can adjust the configuration on your laptop or hand-held and jump onto that network.

Fast as Fast Can Be

Wireless networks are significantly slower than their tangle-able counterparts. While electronics manufacturers are trying to solve this problem, currently the fastest consumer wireless units are 802.11g which theoretically runs 54Mbps. Unfortunately, with the amount of error correction and encryption overhead on wireless connections, real throughput is closer to 20-25Mbps. While this is a mere fifth of the speed of a standard 100Mbps wired network, it will not slow down your broadband connection. Most broadband connections peak downstream speeds are 1.5Mbps, so the speed of your wireless network is only important when transferring files between computers on the local network.

Interference

There are many ways that a signal can be interfered with. Walls in brick homes often block wireless signals, and some cordless telephones and even microwaves can disturb wireless networking connections. This is because of the frequency ranges used by these devices are all near 2.4GHz (gigahertz), and the resonate frequency of water is also near 2.4GHz. Don't worry, you're not going to get microwaved by your wireless access point. To heat water you need a very specific frequency (2450Mhz) that's not used by 801.11. Older microwave ovens and 4.2Ghz telephones may produce microwaves in a range of frequencies several megahertz above and below the key resonating frequency. Some of these frequencies may be used by your wireless network. If you notice that your network connections are dropping when your phone rings or when you're using your microwave, you may need to use a different brand of wireless access point, replace one of your appliances.

Antennas

Any conducting surface or mesh can act as a reflector for some ranges of frequencies. If the spacing in a conductive mesh is less than one quarter of the wavelength of a signal, it will be blocked. (Thank you Michael Faraday, 1791-1867). Those of us old enough to remember VHF and UHF television antennas will remember that they had two sets of horizontal bars, one set spaced further apart than the other. This was to capture the two different frequencies ranges of VHF and UHF. And for you whippersnappers, satellite dishes work with the same principle. The parabolic dish has a wire mesh in it with spacing one quarter wavelength of the frequency it's getting from the satellite and reflects the signal to the collecting head.

How far can it go?

This is the fun part. Standard wireless access points come with simple omni-directional antennas with a max range of about 50 Meters. However, you can put different antennas on your wireless access points to increase the range and the area covered by your access point. You can even build your own antenna out of household materials that will send your signals amazing distances. For example, some solid core electrical wire, a Pringles chips can, and a small coax connector will yield an antenna capable of carrying a wireless networking signal about a kilometer.

Let Me Sum Up

Networking of any type takes time and patience. Some may find that they can just plug the equipment in and it all works without any troubles. Others will find that more research is required before before their network will work the way they want it to. When it is done, and you are web surfing outside by the pool, you will probably consider that time well spent.

Glossary

The most confusing part of any technology for a newcomer is the jargon. Skim over these terms and you will have a much easier time talking about wireless networking.

Wi-Fi

This contraction should stand for "Wireless Fidelity", and while Wi-Fi might sound like Hi-Fi (High Fidelity - meaning highly accurate), this very little to do with the standards of wireless data transmission.

AirPort

Apple often gives more marketable names to technical specifications to more easily present their products to the masses. However, the is used both to describe the access point and the protocol, which may lead to even greater confusion.

802.1x

Here, x is a wild card that is typically 1 or 2. This term refers to all of the following: 802.11a, 802.11b, 802.11g, 802.12, and more.

802.11

The specifications drawn up for wireless computer networking documented by the Institute of Electrical and Electronic Engineers associa (IEEE) in 1996 include a block of the radio spectrum between 2400 Mhz and 2483.5 Mhz (2471-2497 Mhz in Japan). This was the original Mbps version that spurred the more popular a, b, and g flavors.

802.11b

These products actually gained popularity before the a class of products largly due to price. 802.11b has about a 50 Meter omni-direction range and a maximum throughput of 11 Mbps. While, overhead and error correction typically brings this speed down to about 5.5 Mbps, th still five times the speed of the average broadband Internet connection.

NIC

Network Interface Card

Resources:

WarDrive.net

Fake AP

PrismStumbler

IEEE 802.11 Standards Draft

802.11 Wiki