Thief or Freeloader? The Ethics Surrounding Unauthorized Wireless Network Access

By Aaron Stearrett

CSC 300

Abstract

In the past several years, the number of wireless networks has increased dramatically, due to the availability of low-cost wireless networking equipment. Unfortunately, many of these wireless networks are not secured against unauthorized use. In the worst-case scenario, these unsecured wireless networks could allow unauthorized users to access sensitive government or corporate documents. The ethics surrounding unauthorized use of wireless networks are discussed. Specifically, the paper looks at two sides of the issue: the idea that a wireless network's signal is in the public domain and should be accessible to anyone, and the idea that unauthorized use of a wireless network is bandwidth theft. The conclusion is made that unauthorized use of a wireless network is, in fact, bandwidth theft, although wireless network owners should explicitly deny unauthorized use by properly securing their networks.

Introduction

The way people connect to the Internet today has changed dramatically with the rise of inexpensive wireless networking hardware. Unfortunately, these devices are often difficult to configure securely, and as a result, allow anyone with a wireless network card and within range of an unsecured wireless network free access to the Internet by connecting to a neighbor's router. This paper will attempt to separate the technical limitations of wireless networking hardware from the underlying ethical principles surrounding accessing a wireless network without the network owner's knowledge. It will attempt to show that, according to American principles of rights of ownership, it is not ethical for an individual to knowingly access a wireless network unless the owner gives them permission to do so. If, however, a user is forced onto a wireless network by wireless network configuration software and the user does not know he is connected to a wireless network, this paper will attempt to show that the user has not acted unethically.

Facts

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) released the 802.11 specification, which defined a wireless network that ran on the unlicensed 2.4 GHz frequency band. The original specification defined two separate data transmission rates: one and two megabits per second. Two revisions to this standard, 802.11b and 802.11g, increased the throughput to 11 megabits per second and 55 megabits per second, respectively [wiki04].

Today, wireless networks are big business. According to *Computing*, the market value of wireless network equipment was $724 million in 2003, and about 861,700 wireless access points were shipped worldwide [Everett04]. Unfortunately, many of

these networks are not secured. A study performed by the University of South Australia surveyed 729 wireless networks and determined that at least 54 percent lacked encryption. Twenty-six percent of these 729 wireless networks did not even change the set service identifier (SSID) that identifies the name of the router to users of the network [Marr04].

These findings are consistent with the findings from a survey of 1007 wireless networks I conducted on November 6, 2004 in the city of San Luis Obispo. Using my laptop, wireless network card, and a copy of a popular wireless network detection tool known as NetStumbler, I drove around the city of San Luis Obispo looking for wireless networks (See Appendix A for full listing). It should be noted that, during my survey, I did not attempt to read any of the network traffic from these wireless networks, nor did I attempt to connect to any of these networks; I was only able to receive the basic broadcast information transmitted by all wireless networks, including the network's SSID, frequency on which the network ran, wireless router brand, speed of the wireless network, and signal strength. I focused on the student housing areas of the city, although I also surveyed other residential areas of the city. I theorized that the percentage of secured wireless networks would be higher than average in housing areas predominantly serving students, however, statistically, this was not the case. Of the 1007 wireless networks surveyed, 615, or 61%, of these networks did not have any sort of encryption or access restrictions. 324, or 32%, had not changed their SSID. 91 of these 324 wireless routers were made by 2Wire, 32 were made by D-Link, 99 of them were made Linksys, and 72 were made by Netgear. Of these 324 wireless networks with default SSID's, 104 of them had enabled encryption. 86 of these 104 networks used routers made by 2Wire.

According to SBC's web site, the wireless network DSL modems they bundle with their DSL Internet service are made by 2Wire, so it is reasonable to assume that the owners of these routers use the router provided by SBC: the 2Wire HomePortal 1000SW[SBC04]. According to 2Wire's installation manual for the HomePortal 1000SW, all units are preconfigured with encryption turned on. For the user to connect to the wireless router, they must enter the WEP encryption key printed on the bottom of the router[2Wire03]. If routers made by 2Wire are removed from the list, then only 18 of the remaining 233 networks had encryption enabled.

It is interesting to note that, of the 615 unsecured wireless networks surveyed, 395 of them had modified their SSID to a non-default setting. This implies that the owners of these networks knew how to change settings on their wireless router but chose not to. It is also interesting to note that, of the six wireless networks with SSID's such as "Get Your Own Bandwidth", that acknowledge that there are people trying to access their network without their knowledge, only one of them was not encrypted.

Insecure wireless networks such as the 615 I found in my survey can turn into a security nightmare. Using laptops and wireless networking software available on the Internet, individuals are able to read traffic from unsecured wireless networks and retrieve sensitive information such as credit card numbers[Marr04]. Earlier this year, Brian Salcedo plead guilty to a charge that he connected to an unsecured wireless network at a Lowe's hardware store with the intent to steal credit card numbers from their corporate database. The potential loss from this crime, had he succeeded, was estimated at $2.5 million [Poulsen04].

A similar case occurred in Canada in November of 2003. Walter Nowakowski was arrested in Toronto when he was caught downloading child pornography while driving the wrong way down the street. A police investigation concluded the man had been connecting to an unsecured wireless network located near the site of his arrest. He was charged with possession of child pornography, accessing child pornography, distributing child pornography, making child pornography, and theft of telecommunications [Bradley03].

There are also individuals who access wireless networks for less nefarious reasons. Some individuals just search for wireless networks without ever actually connecting to them. There are also some who connect to an unsecured wireless network to get free access to the Internet. I myself connected to several unsecured wireless networks around my apartment before I was set up with my own Internet connection. There are even innocent users who accidentally connect to someone else's wireless network because most computers with wireless network cards automatically connect to the first available wireless network [Dvorak04].

Issue

With the ease that one is able to connect to someone else's wireless network, is it ethical to do so? Should the blame be placed on the users, who many times inadvertently and accidentally connect to someone else's wireless network, or should the burden of securing a wireless network be placed on the owner of the wireless network? What part do the manufacturers play, as wireless network software often automatically connects to a wireless network the user does not even know exists?

Arguments

Not Ethical

There are those that argue that accessing wireless networks without the owner's permission is not ethical and is bandwidth theft. They argue that since the unauthorized users of wireless networks do not pay for the bandwidth they are using without the owner's explicit permission, they are, in effect, stealing it. The people on this side of the argument reject the idea that a network owner implicitly gives anyone permission to access their network by broadcasting its existence, comparing the wireless network to an unlocked or open door [Rist04]. An open or unlocked door is not an implicit invitation for anyone to enter a building, just as an open wireless network is not an implicit invitation to connect to the network. The burden is then placed on the user, who must decide if the network he wants to connect to is open or not. It would, therefore, only be ethical for a user to connect to a wireless network that they knew they had explicit permission to access.

Since an open network is not an implicit invitation for people to access the network, proponents of the argument claim that people who access a wireless network without permission are violating the law and should be punished as criminals. According to section 502.c.7 of the California Penal Code, it is illegal to access a computer network without the owner's permission. Since this permission was not given, accessing the network would constitute a criminal act. The user would also be in violation of section 502.c.5, which prohibits unauthorized access to computer services [Code502]. Because the definition of "computer services" includes computer time and data processing, just connecting to a network would constitute a violation of this section, as a server on the

network needs to assign each user of the network an IP address and route requests to other computers on the network.

Ethical

On the other side of the argument are those who argue that, yes, it is ethical to access someone's wireless network without their knowledge. According to their argument, when the owner of a wireless network broadcasts that the network exists and is available for use, they are giving anyone able to connect to the network permission to connect to that network. The only way to let people know that they do not have permission to access a network would be to enable encryption on the router or enable some other device on the router to prohibit anyone from accessing the network without the owner's knowledge [Dvorak04].

Another common argument used to support this group's claims is the idea that the signal transmitting the wireless network is public domain and should be accessible to anyone able to access it. According to this argument, the person accessing the network is not trespassing on the owner's network or stealing their bandwidth. Instead, the wireless signal and thus the wireless network is trespassing on the person accessing the network. Since this person accessing the network did not give the owner of the network permission to broadcast a network on this person's property, he has a right to access and use it [Dvorak04]. Only if the network is secure should it be considered a private signal and off limits to others. Unsecured networks, however, can be considered fair game to anyone who wants to connect to them.

This way of thinking, say its defenders, makes it easy for users to connect to networks where its owners permit and encourage open access. A user would not have to

take the time to consider if connecting to a particular network could get him in legal trouble. The user would simply connect to the network and be able to use it. The burden of controlling access to any parts of the network would rest upon the network owner. If the owner did not want his wireless network shared, he could enable security on the network and prohibit the user from connecting to it at all [Dvorak04].

One of the other issues pointed to by proponents of this argument is the ease with which a user can accidentally access a wireless network. Consider a Windows user that automatically connects to his own wireless network with a default SSID named "default". If this user uses his computer anywhere there is a wireless network with an SSID named "default", his computer will automatically connect to this network, even if it is not a network owned by him. Proponents of this argument would say that, since he was not able to control whether or not the computer would connect to the network, he has not acted unethically.

Analysis

There are a lot of issues surrounding the arguments for and against accessing wireless networks. The first one that will be addressed is the idea that a wireless signal becomes public domain once it leaves the owner's property and travels elsewhere. I assume that the person who made this argument was stating that wireless signals should legally be defined as public domain, as part of his argument revolved around the legal aspects surrounding the issue I am discussing. Traditionally, any user can use something placed in the public domain without restriction. The problem comes when proponents attempt to place arbitrary restrictions on the signal they claim is "public domain". They claim that, as long as the signal is unencrypted, any user can use that signal in any way

they please. But if the signal is in the public domain, why would it matter if the signal were encrypted or not? Would not anyone in range of the signal still have the right to run an encryption cracking tool on the public domain signal?

There seems, then, to be a contradiction between the term used to describe the principle and the principle itself. Then let us consider, for the sake of argument, that only the unencrypted wireless signals are in the public domain. Vocal proponents of open wireless network access have not traditionally stated that they wish to have access to encrypted wireless networks, so perhaps this more closely approximates their beliefs. That would imply that it was still acceptable to spy on someone else's wireless connection, which would likely violate federal wiretapping laws that prohibit listening in on private conversations taking place through a radio signal. Therefore, wireless signals could not be legally considered public domain.

This argument also assumes that all wireless network transmissions are one-way transmissions. In saying that a wireless network infringes on the user by trespassing on his property is to only discuss half the issue. One must remember that the user must transmit a signal back to the wireless router; therefore, if the network is trespassing on the user, then the user is trespassing on the owner.. If it is the case, as proponents of open wireless access say, that wireless signals should exist where wireless network owners do not want them, then the logic can be turned back around on the wireless network users. If the network owner does not want wireless signals entering his network, then the user should keep his signal away from the owner's property.

One of the most interesting points made by those in favor of open wireless access is the idea that the wireless networking software is partially to blame for the issues

wireless network owners and users face. It is probably true that, in some way, the developers of the software controlling wireless network cards have made it too easy for someone to connect to a network they do not want to connect to. In my own experience with using wireless networks, there have been several instances where I was connected to a wireless network that I did not want to connect to. As I wrote this paper, I was somehow connected to a wireless network with the SSID "default" even though I have never configured my computer to automatically connect to a wireless network with that SSID.

In this regard, software developers have been quite negligent. The software allows a connection to a network which may not be the network a user expects to connect to, then allows the user to transmit potentially sensitive information over the network. This is a pretty large violation of section 1.03 of the Software Engineering code of Ethics, which says that software should only be released if it does not diminish privacy [SCOE]. Automatically connecting a user to a wireless network that may not be a trusted network would certainly be considered a potential violation of privacy. The network could potentially have some kind of packet sniffing software installed to read sensitive information transmitted over the network. Developers could also be in violation of section 1.04, which requires disclosure to user any potential danger to them. Although much attention has been paid lately to wireless network security and the dangers of connecting to an unsecured wireless network, there are still very few warnings in the Microsoft Windows wireless network connection utility. Although the software warns the user the first time they try to connect to an unsecured wireless network, it never displays this message after the software is configured to connect to a network with the

same SSID, even if it is not the same network. At the very least, the software should display this warning every time a user tries to connect to an unsecured wireless network. A more sensible solution, though, would be to modify the way in which the wireless network configuration software decides whether or not the computer connects automatically to a wireless network.

Although Windows systems no longer seem to automatically connect to the first available wireless network, there are still problems that software developers need to resolve before users can be confident they are connecting to the network they want to. While it is a logical choice to connect to a network based on its SSID, the software should base its decision of whether or not to automatically connect to a network on more than just the SSID. Since about a third of all wireless networks use the default SSID, it is not wise for the wireless networking software to automatically connect to a network whenever it has a particular SSID. A more sensible approach would be to store several identifiers for each wireless network it is set to automatically connect to. For example, the software could store the network's SSID, the router's MAC address, the channel on which the network transmits, and the name of the router's manufacturer. These are all pieces of information that can be obtained from a wireless network without connecting to the network, and the four of them combined could provide a profile for each wireless network that would have to match exactly before the computer would automatically connect to a network. Using the wireless router's MAC address would be especially useful, as very rarely do two wireless routers have the same MAC address. In my survey of 1007 wireless networks around San Luis Obispo, no two wireless routers had the same MAC address. Although it is possible for a user to change their MAC address and SSID

to match another router, the probability that this will happen is lower than two networks simply having the same SSID. If this solution were coupled with a warning message every time the software tried to automatically connect to a wireless network, the user would be able to verify that he was within range of his own network, as two networks with the same SSID and running on the same channel must be out of range of each other.

But the question remains: do the deficiencies in the wireless network configuration software cause accessing someone's wireless network without their knowledge to be an ethical act? When a piece of software chooses to automatically connect to a wireless network, it has taken control away from the user. It has, in effect, taken the decision away from the user, and placed the user in an ethically ambiguous position where the user must actively decide to disconnect from the network instead of actively decide to connect to the network. The software, then, could be seen as authoritative in regards to connecting to wireless networks. It seems logical to accept this software's authority in regards to connecting to wireless networks. After all, the user would be unable to connect to a wireless network without the software. When the software decides to arbitrarily connect to a wireless network, it is exerting this authority.

Milgram's famous study on the effects authority has over an individual's ethical standards demonstrates the effect this authoritative program can have on a computer user. As people tend to give into authority and simply follow the wishes of an authoritative figure[Wade02], people who accept software's authority to act correctly might not question the ethical implications of their computer connecting to someone else's wireless network. They may just assume that since the software is connecting them to someone's

wireless network, then this behavior must be acceptable. After all, why would a company release a piece of software that did something illegal or unethical?

If, on the other hand, the network configuration software popped up a dialog box warning users that it was potentially illegal for them to connect to a wireless network they did not have permission to access, the casual user would probably be less likely to connect to someone else's network for the same reason they would be more likely to not disconnect from a network their system has already connected to. The software would be seen as an authoritative figure, and the user would not want to do something that their computer warned them was potentially unethical or illegal. Thus any position taken by this piece of software seen as authoritative could have a large impact on how the user acts when faced with this ethical dilemma. Based on the aggressive action wireless networking software takes in regard to automatically connecting to wireless networks it could reasonably be concluded that the wireless network configuration software contributes to the behavior of connecting to a wireless network the user does not own or have permission to use. Since the software takes such an active role in connecting to these networks, the user becomes an accessory to what the computer is doing instead of telling the computer what to do. The user may reap the benefits of what the computer has done, but it was not the user who connected to the wireless network; it was the computer. And since it is often not made apparent what the computer is doing when a wireless network card is plugged into a computer, how can the user be faulted?

I find the situation analogous to a driver and a passenger in a car. The driver decides to drive around where he is not allowed, but the passenger does not know they are not allowed to be where they are. If the passenger does not ask the driver if they have

permission to be where they are, has the passenger acted unethically? No, because the passenger does not have a responsibility to know where the driver is and is not permitted to drive; the driver is. The driver is in charge; the driver has a responsibility to only drive where he is allowed. The passenger is just that, a passenger. Ethically, since he was not the one who violated the law and had a reasonable assumption that they were not violating the law, he should be in the clear. So it is with wireless networking software. When the software takes control of connecting to wireless networks automatically, it also takes the responsibility to only connect to networks it is authorized to connect to. The user, then, should be ethically absolved of responsibility for the computer's actions if he does not suspect the computer of wrongdoing.

Let us then assume that this issue is eventually resolved. Wireless network configuration software no longer works in a manner that gives users the belief that connecting to someone's wireless connection without their consent is ethical. Is it now ethical to access someone's wireless network without their knowledge? People on the affirmative side of the argument still argue that it is the owner of the wireless network's responsibility to secure their wireless network. This assumes, though, that the manufacturer of wireless networking equipment has done their part to make it easy for a user to secure their network. The Software Engineering Code of Ethics says that engineers should "strive for high quality, acceptable cost, and a reasonable schedule, ensuring significant tradeoffs are clear to and accepted by the employer and the client, and are available for consideration by the user and the public."[SCOE] In the wireless networking field, this could mean that engineers properly weigh the tradeoffs between security and ease of use. Section 1.03 states that engineers should "approve software

only if they have a well-founded belief that it is safe, meets specifications, passes appropriate test, and does not diminish quality of life, diminish privacy or harm the environment."[SCOE] The corollary to the wireless hardware world would be that the network is sufficiently secure out of the box, so that a user who did not know how to configure their network would have a reasonably secure network. Section 1.05 of the code states that engineers should "cooperate in efforts to address matters of grave public concern caused by software, its installation, documents, methods and tools."[SCOE] With this in mind, do the manufacturers of wireless networking equipment do their part to ensure that their hardware is secure so that the people who buy this equipment can responsibly secure their network?

Looking at the number of unsecured wireless networks that exist suggests that hardware manufacturers do not ensure that their hardware is secure before they ship it to consumers. I do not have figures on the number of wireless routers that have encryption enabled by default, but I do know that neither of the two wireless routers I own had any sort of security enabled by default. To enable security on my wireless network, I had to type in a 26 digit WEP key in five different places: once in my router, twice in my laptop, and once in my roommate's laptop. I was also unable to see if I was typing this 26 digit key correctly into my computer, as the Windows network configuration utility treats the key as a password and conceals it under asterisks. I also know that both of these routers had administrator usernames and passwords of "admin", which means that anyone accessing one of these routers in a default-configured state would be able to log into the administrator page and take control of the router.

It would seem that the tradeoffs the engineers of this equipment made sided too much on the ease of use end of the spectrum and not enough on the security end. While it is understandable that manufacturers do not want to be swamped with support calls from users unable to access their network due to the network being too secured by default, it would not be difficult for a company to add some increased security to their default configurations.

Let us consider the default configuration in the 2Wire routers SBC ships their DSL customers as part of their home networking kit. Recall that these routers are shipped with WEP encryption turned on by default, and that I only found four of these routers with WEP turned off. To access this network, the owner must find the default WEP key and the router's serial number, both located on stickers on the bottom of the router. To use the router, the owner must type this WEP key into the wireless configuration utility. The user selects the wireless network with the SSID "2Wire" followed by the last three digits of the serial number found on the bottom of the router.

This company has chosen the opposite end of the spectrum, and has apparently met with decent results. Granted, this is not an optimal solution to the larger problem of creating secure, default routers; but it can serve as a lesson on how few users chose to run unsecured wireless networks when they are given a secure network by default. We could possibly go a step further and guess how many people would voluntarily run a open, unsecured network if they were given the choice

If it is true that wireless network owners, for the most part, accept their routers's default security settings, then the very ease of use of wireless networking software on the client end suggests that wireless network owners should not be wholly responsible for

securing their networks until default security allows them to do this easily. As the manufacturers have failed in their duty to give their users the ability to easily secure their network, how can the user be entirely responsible for his network? The original premise at this stage of the argument was that the software controlling wireless network clients was fixed. That is, wireless network connection utilities no longer hold a position of authority over the user. The software only connects to networks the user wants to connect to. At the present, this user cannot assume that the owner of a network has made the conscious decision to not secure his network, and thus cannot assume that the owner is willing to share his network connection with people he does not know. As the user cannot assume that he has permission to access this network, it would not be ethical to access their network according to deontological reasoning.

Deontological reasoning teaches that an individual should not use another individual merely as a means to an end [Johnson02]. As such, people should refrain from using others merely to advance their own goals and ambitions. To connect to someone's wireless network without first asking permission or allowing them to deny users access to their wireless network would be treating the owner as a means to an end, where the end is free Internet access. The argument could be made that the owner has the ability to deny users access to their wireless network by securing it. However, as was discussed earlier, wireless routers at present do not give owners the ability to easily assert their right to deny access. As it is important in deontological thinking that an individual be able to assert a rational decision easily, one cannot assume permission to use a resource is given if it is too difficult for the owner of this resource to deny this permission.

Let us assume, then, that it is not difficult for an owner to secure their wireless network. Let us assume that wireless hardware manufacturers require that owners of wireless networks choose whether or not to secure their wireless network, and let us assume that all wireless network owners fully know the consequences of not securing their network. Is it then ethical to access someone's wireless network without their knowledge?

Central to the deontological argument before was the idea that the owner of a wireless network could not easily deny someone access to his network. However, we never discussed if not denying access to the network constituted permission. I am going to argue that it does not. Just as it is possible but not necessary to secure property in the physical world and have an expectation that it will not be used or taken, there should be no requirement to secure a wireless network in order for it to be private. That is not to say that a wireless network should not be secured, just as it would be foolish, for instance, for an individual to not secure their car while in a bad part of town.

In the physical world, there are laws against unauthorized access to private property. Although I do not want to get into the legalities of accessing a wireless network without the owner's permission, the law can be used as a template to see what rights a property owner has over his property and what, if any, responsibilities the owner has to secure his property. California Penal Code section 602 lists many situations which are considered trespassing. The principle behind these laws seems to be that it is not ethical to enter someone else's property without permission when it is known that the property is private, and it is unethical to refuse to leave the private property once asked by the owner or law enforcement. Although most of the laws regarding trespassing

require specific damage to be done to the property, there are several laws that suggest that the mere act of using private property without malicious intent to be unethical. The only requirement on the part of the owner is that he make a reasonable effort to let others know that the property is private. There is no requirement that the owner erect a fence around his property or secure it in any way [Code602].

In the wireless network world, there are some parallels to the ethical principles behind this law. The private property becomes the wireless network and the bandwidth used to connect this wireless network to the Internet. When an individual pays for an Internet connection, they are paying for the bandwidth that their Internet Service Provider will provide them in order to access the Internet. He has also paid for the wireless router, has configured it by his own labor, and pays for the electricity to power its wireless transmission. Thus, the wireless network and its connection to the Internet become his property.

The act of making it know that the network belongs to someone is simple, as the wireless network does this automatically. The fact that wireless networks do not exist in nature implies that someone owns the wireless network. What constitutes permission? There are several ways the owner of a wireless network can give a user permission to use the network. One way would be for the user to ask the owner for permission verbally or in writing. Another way would be for the user to pay for the wireless network connection, as some coffee shops such as Starbucks do. Or the owner could make it known by modifying the SSID that he does not mind other people using his wireless connection. An SSID of "open access" or "free wireless" would probably be sufficient to announce that anyone is permitted to access a wireless network. Just having a wireless

network unsecured does not constitute permission because it is not explicit permission to use the network. There could conceivably be a reason in this highly idealized situation where the owner of a network would not want to share an unsecured network. As long as there is the possibility that a network owner would choose to not secure his private wireless network, and as long as there is no requirement that a property owner secure his property against theft, the assumption cannot be made that an unsecured wireless network is a public wireless network.

It also does not matter if the user is able to access my wireless network from his property. There are many instances in the physical world where one person's property encroaches on another's. A good example of this is the power meters installed on houses. Although they are installed on someone else's property, there is still the expectation that they belong to the power company and should not be tampered with. The homeowner cannot, for example, change the reading on the meter, nor can he take it with him when he moves. So it is with a wireless network that is accessible from someone else's property. Although it does transmit to another person's property, the owner does not lose his claim of ownership of that signal, as it is being transmitted by property belonging to the owner. And even if property of the signal itself was transferable, ownership of the bandwidth the network is connected to would not be transferred, as it is not being transmitted by the wireless router. The only property that would be transferable would be the signal broadcast by the router that lists such things as the router's SSID, MAC address, and router manufacturer.

The argument was given earlier that when a user accesses a wireless network without the permission of the network owner, it is bandwidth theft. When I buy my

Internet connection from SBC, I am paying for a set amount of bandwidth that I am allowed to use. In my case, I get a three megabit per second connection. This is sufficient when I split the connection between myself and my three roommates. What happens, though, if someone else connects to my network and downloads a large file? I am deprived of my property, as some of the bandwidth I have paid for has been taken in such a way that I am no longer able to use it. I have, in effect, been deprived of something I have paid for by someone who has not asked my permission to deprive this bandwidth from me. Since I do not have this bandwidth that I paid for, and since this other person is using this bandwidth he did not pay for, he has stolen my bandwidth. It does not matter whether or not my network was secure; this individual has chosen to connect to my network without my permission and use it for his personal gain.

In light of this, it is not even an innocent act to knowingly access someone's wireless network without their consent. If it were an innocent or harmless violation, one could possibly make the argument that it was ethical because it does not cause damage to the owner's property. At the very least, accessing the network could be seen as violating the letter of property rights but not the spirit. But it does cause harm by lowering the quality of service on the network. In some cases, it can cause greater harm than simply lowering quality of service. In one particular published case, a company's Internet bill increased from about $5000 per quarter to about $3000 in a week due to unauthorized access to their wireless network [Marr04]. This is far from a harmless ethical violation. Even if none of the people who used this wireless connection used it excessively, many people accessing this network in a period of time could cause the amount of bandwidth used to increase.

From a utilitarian point of view, this could be seen as an argument against accessing the network. Utilitarianism argues that each individual's actions should increase the total amount of happiness[Johnson04]. Let us assume that, before a user connects to a wireless network, everyone is at their baseline level of happiness. We will consider this baseline happiness sum as zero, which means each individual is neither happy or unhappy. An unauthorized user connects to a wireless network. His happiness has increased because he has free access to the Internet. The owner's happiness has decreased because the amount of bandwidth he has available to use has decreased Now, consider if another wireless user connects to the network. His happiness increases by a certain amount but the total amount of bandwidth available to everyone else decreases, decreasing the happiness of the other two people connected to the network. The first user's happiness will still probably be higher than it was before he connected to the network, but it will not be as high as it was before the second user connected and decreased the available bandwidth. Now let us consider that enough people connect to the network that there is no longer enough bandwidth for the network to properly function. As the network is now no longer functioning, the level of happiness of the unauthorized users should drop back down to zero. It may be less than it was at the baseline, as the frustration gained from once having a working Internet connection and no longer having one could have decreased happiness below what it was when they had no Internet connection at all. However, assume that the network is only so slow as to drop the users' happiness back down to its base level. The happiness of the users will all be zero and can be cancelled out, leaving only the happiness level of the network owner. As he could not have foreseen his network becoming slowing to a crawl due to unauthorized

users connecting to his network, we can be fairly confident that this will decrease his level of happiness in relation to its base level. If he will be required to pay more in Internet connection fees, his level of happiness will be even less.

Looking at that scenario, there would seem to be a relative maximum level of happiness that exists when the sum of the unauthorized users' level of happiness is greater than the level of unhappiness of the network owner. However, without being able to see the big picture, it would be impossible to determine how many unauthorized users would be required to maximize the happiness of everyone. As an individual user is unable to determine how much the total happiness will change as a result of connecting to network, the safe conclusion would be to not connect to the wireless network. There are too many unknowns regarding the levels of unhappiness of others to logically conclude that it would increase the total amount of happiness by connecting to the network. Since it is worse to decrease the total amount of happiness than it is to leave it constant, the correct decision would be to not connect to the network.

Conclusion

Having said all this, it is still possible to get free wireless Internet from someone; it just requires that the owner give their permission. This can be accomplished by knocking on their door and asking them. Although it is sometimes difficult to pinpoint where a wireless router is located, sometimes clues are given as to its location. Several of the SSID's of wireless networks I found had address information. Others use the owner's name as an SSID. This is the approach I take with my wireless network. The more technically-minded could use a program such as NetStumbler to walk around with a laptop and monitor the signal strength. The area surrounding the house or apartment with

the strongest signal strength usually has the router. At the very least, the owner will say no. However, the owner might also say yes. Even if the owner says no, the owner might come to the realization that his network is accessible to other people and take steps to secure it.

Aaron 00:12:17:12:c7:90 secure
NETGEAR 00:09:5b:dd:35:cc unsecured
BatPod 00:0c:41:f7:8c:e2 unsecured
711 00:06:25:06:13:96 secure
default 00:0d:88:2f:de:c9 unsecured
linksys 00:0f:66:ad:0b:59 unsecured
CD705B 00:0f:3d:3e:40:68 secure
megan 00:0f:66:c2:09:14 unsecured
linksys 00:0f:66:39:38:22 unsecured
Mustang605 00:0f:66:bb:3d:0e unsecured
Holmes Network 1 00:12:17:0b:e5:62 secure
envy 00:0f:66:c1:c4:c4 secure
aquafinagurl 00:0f:66:94:0f:c4 secure
NETSLO 00:09:5b:af:46:a8 unsecured
linksys 00:0f:66:ad:0b:5c unsecured
asian fever 16 00:06:25:8d:09:cb secure
monkeys 00:06:25:b4:1e:79 unsecured
slocal 00:06:25:88:7f:65 secure
linksys 00:12:17:0e:a4:47 unsecured
bigtyme 00:0f:66:bb:25:ba secure
hellapimp 00:0f:66:8c:13:f7 unsecured
606 00:0f:66:ca:e9:89 unsecured
Soccer 00:12:17:0c:37:1c secure
NETGEAR 00:09:5b:ed:4a:94 unsecured
Paul's Wave 00:09:5b:d9:07:c8 unsecured
default 00:0f:3d:35:ea:e7 unsecured
gilligan 00:0f:66:bb:0d:ce secure
Drekol 00:0d:88:bc:35:1d secure
belkin54g 00:30:bd:95:75:df unsecured
linksys 00:0f:66:c3:19:36 secure
Router 00:09:5b:6e:a8:d0 secure
EVANGELION 00:09:5b:70:41:fa secure
2WIRE650 00:0d:72:92:6b:99 secure
Route 00:06:25:60:70:97 secure
Hi 00:09:5b:cf:6e:08 unsecured
Richard 00:09:5b:fa:8c:16 secure
brians_wireless 00:09:5b:5e:41:ef unsecured
SMC 00:04:e2:83:cc:64 unsecured
00:0f:66:ca:e9:81 secure
2WIRE166 00:d0:9e:d8:e5:e1 secure
neurotonic 00:0f:66:d8:12:ae secure
02:00:60:4c:e1:00 unsecured
00:0f:66:c6:12:10 secure
KC 00:11:24:03:bd:ad secure
AsianGangstas 00:09:5b:ca:bf:1e unsecured
RevolveASL 00:0f:3d:49:cc:2c secure
02:00:f5:a9:45:10 unsecured
02:00:5f:cb:1c:14 unsecured
ROFLCOPTER 00:0f:3d:3b:09:6c unsecured
301girls 00:0f:66:aa:c5:8d secure
ecsyrtis' hub 00:0f:66:aa:c5:8f secure
MustangWireless 00:11:21:fd:1e:b0 unsecured
02:00:5b:2b:f4:17 unsecured
02:00:75:12:cb:1b unsecured
109mustang 00:12:17:0b:5d:ff secure
2WIRE664 00:0d:72:9c:af:11 secure
central intelligence 00:11:24:02:ff:b9 secure
KN Entertainment 00:0c:41:c0:3c:f9 unsecured
02:00:fd:2f:a2:1f unsecured
02:00:36:51:79:23 unsecured
gerbilwlan 00:0c:41:c6:1e:8b secure
WEPpls 00:12:17:04:0b:df secure
martin 00:0c:41:4a:11:66 secure
NETGEAR 00:09:5b:ed:b3:7e unsecured
Piqui 00:06:25:7f:f0:df secure
Mustang Lab 00:0f:66:02:11:ef unsecured
FlyingCow 00:0f:66:a4:12:bd secure
2WIRE902 00:0d:72:77:c3:d1 secure
linksys 00:0f:66:b9:84:44 unsecured
theroost 00:09:5b:ea:a1:24 secure
00:0d:72:97:aa:c1 secure
funny 00:09:5b:fa:f6:9e unsecured
Hayley 00:09:5b:6f:07:be secure
TERIYAKI 00:0f:66:c6:12:e2 secure
2WIRE129 00:0d:72:1e:60:f9 secure
ournetwork 00:0f:66:8c:31:31 secure
linksys_TT 00:03:2f:01:23:bb unsecured
linksys 00:0c:41:47:9a:d8 unsecured
linksys 00:0f:66:cb:03:21 unsecured
2WIRE236 00:0d:72:84:b9:31 secure
linksys 00:0f:66:0c:5a:41 unsecured
OURS 00:0f:66:aa:c5:8b secure
belkin54g 00:30:bd:f0:81:03 unsecured
linksys 00:0f:66:ad:4a:e9 unsecured
Sambo 00:06:25:f4:ff:01 secure
NETGEAR 00:09:5b:d6:b4:b8 unsecured
00:0f:66:49:6d:0c unsecured
linksys 00:0f:66:56:81:c3 unsecured
linksys* 00:0f:66:ba:52:e5 unsecured
2WIRE855 00:0d:72:9c:f8:69 secure
DIGITALFORTRESS 00:0f:66:d7:e3:fe secure
Mia Sorensen 00:11:24:04:53:fd secure
00:09:5b:4d:e2:98 secure
tandum 00:0f:66:c3:3e:d7 secure
default 00:0f:3d:5b:75:fe secure
WLAN 00:30:bd:c1:0c:f2 unsecured
f00 00:12:17:09:8b:3a secure
HI 00:0f:3d:40:98:da unsecured
Suck It Bitches 00:0f:66:c3:b1:70 secure
NETGEAR 00:09:5b:71:43:fa secure
JJ 00:0f:66:e3:ec:0a secure
alpha 00:06:25:f2:ca:39 unsecured
steely dan 00:0f:66:c3:b6:b0 secure
unit97 00:06:25:fa:f3:cd unsecured
AEPi 00:0f:66:bc:72:2d unsecured
NETGEAR 00:09:5b:fc:9a:c6 unsecured
linksys 00:0f:66:05:97:98 unsecured
Athena8zeus 00:0f:66:a1:14:e1 secure
linksys 00:12:17:04:0f:66 unsecured
lolipop 00:0f:66:9b:e8:83 unsecured
Nazgul Wireless 00:09:5b:fa:41:68 unsecured
linksys 00:0c:41:b7:62:cc unsecured
linksys 00:0f:66:8e:ae:6f unsecured
Raven 00:30:ab:1b:d0:b9 secure
ganda 00:0f:66:74:fe:82 secure
linksys 00:0c:41:71:8c:7a unsecured
Evan 00:0f:66:a7:8d:33 secure
02:00:56:3e:44:a2 unsecured
linksys 00:0f:66:29:6b:e7 unsecured
304 00:0d:88:3f:88:39 secure
digitalputty 00:02:2d:0d:d2:28 unsecured
Buffalo 00:0d:0b:1a:e7:a7 unsecured
Controller 00:0d:72:93:3d:41 secure
default 00:00:94:d4:d8:eb unsecured
MSHOME 00:50:f2:75:3f:78 unsecured
Spike 00:0c:41:79:b2:94 unsecured
2WIRE805 00:0d:72:00:c7:79 secure
2DayULook 00:0f:66:d7:f2:b3 unsecured
linksys 00:0f:66:ad:02:bc secure
cada 00:0f:66:0c:18:77 secure
WIRELESS 00:09:5b:95:52:96 unsecured
2WIRE845 00:0d:72:9d:5f:f9 secure
MSHOME 00:0d:3a:29:e7:98 unsecured
GoAway 00:09:5b:ca:ff:16 secure
Mariano 00:0f:66:05:47:2f secure
default 00:0d:88:1d:54:76 unsecured

linksys 00:0f:66:c3:ce:17 unsecured
2WIRE335 00:0d:72:92:7a:39 secure
James is hot 00:0f:3d:51:43:da secure
Hot Girls 00:12:17:01:9d:b6 secure
linksys 00:0f:66:9f:bb:85 unsecured
helpme 00:0f:66:66:5e:bc secure
MustangWireless 00:02:8a:42:2e:10 unsecured
MustangWireless 00:0d:28:9c:c7:e6 unsecured
MustangWireless 00:40:96:40:4e:0a unsecured
MustangWireless 00:40:96:40:6b:a6 unsecured
MustangWireless 00:0c:ce:33:32:27 unsecured
CalPolyWireless 00:60:1d:f1:48:46 unsecured
MustangWireless 00:40:96:41:1c:b4 unsecured
00:50:f2:cb:4e:ae secure
linksys 00:0c:41:cb:a0:17 unsecured
Yikes 00:30:65:2c:d3:7c unsecured
telco21 02:d9:b4:68:c6:c1 secure
telco21 02:84:d3:35:a1:9c secure
NETGEAR 00:09:5b:db:d9:4e secure
hpsetup 02:5e:c4:b8:75:c6 unsecured
Wireless Network 7a:c3:a0:3f:58:d6 unsecured
00:09:5b:6e:cd:ce secure
02:00:0d:4f:81:25 unsecured
02:00:c8:6d:58:29 unsecured
Wireless Network 02:0e:35:08:7f:8b unsecured
ANY 02:04:23:b1:37:37 secure
Wireless Network 12:d8:ff:25:c9:e8 unsecured
00:09:5b:dd:41:ac unsecured
MustangWireless 00:40:96:57:66:30 unsecured
skyriver 5e:0e:88:e4:f6:55 unsecured
huxley 02:0e:35:33:22:20 unsecured
boron 9e:f3:23:43:1b:9b secure
tsunami 02:04:23:7c:81:93 unsecured
skyriver a2:74:aa:43:ef:be unsecured
skyriver 5a:d2:9f:5b:1c:20 unsecured
linksys 02:0e:35:00:00:80 unsecured
POD 02:01:6e:41:e8:5d unsecured
00:00:00:00:00:00 unsecured
skyriver 00:12:17:0e:75:82 unsecured
hpsetup 02:00:f1:b0:50:9e unsecured
hpsetup 02:00:cf:27:28:a2 unsecured
Sammy Hatae's Computer 92:d5:f6:a0:66:b2 unsecured
PIERCENET 00:06:25:a1:87:a2 secure
telco21 02:f0:b5:41:c7:e8 secure
telco21 02:9d:13:2c:61:85 secure
MustangWireless 00:0c:ce:91:cd:85 unsecured
piratesof#19 00:0c:41:41:14:34 secure
linksys 00:06:25:db:b2:3b unsecured
linksys 00:0f:66:9b:e8:09 unsecured
Wireless G 00:09:5b:fb:78:38 secure
netgear10 00:09:5b:ff:66:4a unsecured
linksys 00:0c:41:ca:88:6f unsecured
linksys 00:0c:41:43:29:e4 unsecured
2WIRE438 00:0d:72:93:62:09 secure
linksys 00:0f:66:4d:fe:27 unsecured
2WIRE280 00:0d:72:99:77:09 secure
VickiSchool 00:0f:66:48:22:de unsecured
2WIRE769 00:0d:72:66:76:31 secure
wheresmytux 00:0c:41:45:2b:f4 unsecured
2WIRE899 00:0d:72:92:4f:19 secure
ATMOSPHERE 00:0f:3d:4a:ec:fc secure
linksys 00:0f:66:ad:02:b6 unsecured
linksys 00:06:25:e6:6f:7d unsecured
linksys 00:0f:66:9b:6c:4b unsecured
linksys 00:0f:66:9a:f0:b5 unsecured
Princesses 00:30:bd:c4:74:cc unsecured
2WIRE839 00:d0:9e:d8:4c:b1 secure
295C 00:09:5b:6a:3c:cc unsecured
WARCRAFT 00:09:5b:dd:7a:2e unsecured
linksys 00:0c:41:4a:50:1c unsecured
WaldoWireless 00:c0:49:e0:80:2e unsecured
2WIRE142 00:0d:72:65:5f:41 secure
Walter 00:09:5b:c4:90:cc secure
2WIRE028 00:0d:72:1e:2c:89 secure
wireless 00:90:4b:60:00:2c unsecured
linksys 00:0f:66:05:93:c6 unsecured
674 Foothill 00:0f:66:cb:03:2d unsecured
linksys 00:0f:66:a9:f5:1b unsecured
Freedomlink 00:0f:8f:71:2d:a0 unsecured
2WIRE879 00:0d:72:67:85:21 secure
2WIRE819 00:0d:72:77:c9:b9 secure
linksys 00:0c:41:42:d5:44 unsecured
NETGEAR 00:09:5b:dd:82:58 unsecured
FBI 00:09:5b:51:ad:40 unsecured
Vince 00:12:17:09:eb:8b secure
AllisonCourtney 00:12:17:02:da:51 secure
linksys 00:0f:66:56:51:43 unsecured
Wolf 00:0d:72:8e:ab:49 secure
linksys 00:0f:66:38:59:74 unsecured
Christians 00:09:5b:9b:2a:34 secure
linksys 00:0f:66:49:9d:5a unsecured
Hammonds 00:60:b3:6f:54:87 unsecured
00:0f:66:23:b3:13 unsecured
00:0f:66:52:c0:ea secure
Stormy1 00:50:f2:c7:c7:ae secure
buildersplus 00:12:17:12:c7:81 unsecured
Durango 00:0f:66:d7:e6:4a secure
NETGEAR 00:09:5b:c6:79:e6 unsecured
Bebop 00:40:05:25:25:f3 secure
GodBressYou 00:12:17:0b:e5:59 unsecured
NETGEAR 00:09:5b:50:c1:da unsecured
thepreservationhall 00:12:17:02:da:54 secure
TSUNAMI 00:0f:66:ca:ea:23 secure
00:0e:84:4b:15:da secure
default_d-link 00:40:05:ca:4a:0e unsecured
meike 00:06:25:0f:5f:48 unsecured
jazmine 00:0f:66:ad:f4:cf secure
linksys 00:0f:66:ca:e9:99 unsecured
00:09:5b:f7:a4:50 secure
The_One 00:09:5b:fb:8e:02 secure
meike 00:06:25:0f:63:a5 unsecured
intarweb 00:09:5b:50:97:56 secure
GO_SLO 00:09:5b:fb:cf:88 secure
Mr_Mambaje 00:0c:41:79:34:e2 unsecured
shark 00:06:25:88:c8:bd unsecured
misunderestimated 00:0f:66:9b:77:bf secure

Wireless 00:09:5b:3e:09:c6 unsecured
Fuck You 00:0f:3d:06:9e:31 secure
tayler 00:0c:41:48:30:74 unsecured
default 00:0d:88:bf:67:d7 unsecured
SexyFencers 00:0f:66:ca:e9:83 secure
Alpine 00:09:5b:86:9e:da secure
linksys 00:06:25:fb:f2:84 unsecured
00:0c:41:48:30:7c secure
TheBoach 00:0f:66:39:80:88 secure
bmwcobra 00:0f:66:c3:b6:b6 secure
Clan Wolf 00:90:4b:3a:6b:b8 secure
default 00:80:c8:b0:bd:80 secure
00:0f:66:c6:11:ec secure
00:30:bd:ca:93:2a secure
linksys 00:0f:66:8f:16:fa unsecured
linksys 00:0c:41:b9:e6:e8 unsecured
00:0e:84:4b:15:d3 secure
linksys 00:0f:66:63:30:87 unsecured
NETGEAR 00:09:5b:53:b4:80 unsecured
195 00:0c:41:42:d6:6c unsecured
NETGEAR 00:09:5b:6f:aa:44 unsecured
Degoba System 00:0d:3a:6e:49:db secure
linksys 00:0c:41:72:8a:ae unsecured

wireless 00:0d:88:89:3c:2d secure
linksys 00:06:25:e7:d5:cd unsecured
linksys 00:0c:41:3c:e4:dc unsecured
linksys 00:0f:66:2f:d1:a9 unsecured
linksys 00:0f:66:8e:ae:4e unsecured
NETGEAR 00:09:5b:6f:90:30 unsecured
DelSur 00:09:5b:dc:04:ba unsecured
delsur161 00:0c:41:42:d6:46 secure
jcnet 00:12:17:04:0f:87 unsecured
linksys 00:0f:66:c4:31:9e unsecured
Gateway 00:e0:b8:6b:bb:6e unsecured
linksys 00:0f:66:c3:1e:c7 unsecured
default 00:05:5d:ed:23:c0 unsecured
digitalputty 00:02:2d:93:9b:7b unsecured
paul 00:0f:3d:43:8f:08 secure
wireless 00:90:4b:3c:21:64 unsecured
myadidas 00:0d:88:88:46:5d secure
linksys 00:12:17:04:0f:7b unsecured
linksys 00:06:25:e5:da:03 unsecured
NETGEAR 00:09:5b:c2:3d:e4 unsecured
00:0f:66:aa:72:8b secure
00:0d:72:9c:07:41 secure
linksys 00:0c:41:49:ee:0e unsecured
linksys 00:06:25:88:e4:07 unsecured
2WIRE870 00:0d:72:6a:cb:41 secure
default 00:0f:3d:3f:f0:e2 unsecured
WLAN 00:01:24:f1:cf:35 unsecured
2WIRE753 00:0d:72:9c:a2:f1 secure
linksys 00:06:25:66:9b:dc unsecured
NETGEAR 00:09:5b:6a:79:d2 unsecured
brainstorm 00:0d:88:1e:b4:3a secure
Casa Maria Wireless Mac Network 00:0d:93:cb:02:eb secure
beerland 00:0f:66:74:fb:fe secure
grizzlybear 00:09:5b:fa:f2:86 secure
default 00:0d:88:20:4e:02 unsecured
NETGEAR 00:09:5b:cd:ee:76 unsecured
pearce 00:0c:41:b7:2a:8c secure
00:04:5a:0f:0e:e8 secure
linksys 00:0f:66:39:f0:4e unsecured
NETGEAR 00:09:5b:6a:51:10 unsecured
default 00:0d:88:a1:52:23 unsecured
00:60:1d:f0:d0:be secure
linksys 00:06:25:54:c4:2c unsecured
11xJaHaaYx03 00:0c:41:ac:f4:4f secure
linksys 00:0c:41:66:49:a9 unsecured
00:40:96:28:fa:45 unsecured
linksys 00:06:25:f1:7a:e4 unsecured
00:0c:41:a0:31:ba unsecured
linksys 00:06:25:a1:e8:ee unsecured
JessicaWireless 00:0c:41:b1:fe:84 unsecured
COWPOLY 00:09:5b:fa:23:7e secure
DoctornutzWiFi 00:0f:66:2b:53:79 secure
default 00:0d:88:a0:14:25 secure
linksys 00:0c:41:3c:a9:10 unsecured
NETGEAR 00:09:5b:9f:1a:56 unsecured
NETGEAR 00:09:5b:6e:a8:96 unsecured
00:0f:66:aa:ea:93 unsecured
2WIRE287 00:0d:72:86:f1:51 secure
HOME 00:0f:66:c3:a3:5d secure
linksys 00:0f:66:01:6d:8e unsecured
SLONET 00:0d:88:9a:6a:7c secure
NETGEAR 00:09:5b:c8:a4:5c unsecured
2WIRE365 00:0d:72:53:e9:91 secure
linksys 00:0f:66:56:69:f9 unsecured
default 00:0f:3d:3a:c8:8e secure
skimboard 00:0f:66:d7:f9:13 secure
00:06:25:76:52:af secure
101 00:06:25:e7:cd:cd secure
00:0d:72:86:62:79 secure
NETGEAR 00:09:5b:d9:15:fc unsecured
NETGEAR 00:09:5b:af:46:a6 unsecured
Hansen 00:0f:66:d7:bc:83 secure
BLTM 00:40:05:cb:68:70 secure
linksys 00:0f:66:9f:bb:81 unsecured
default 00:0f:3d:40:95:24 unsecured
Home 00:0f:66:ca:e9:01 unsecured
2WIRE397 00:0d:72:8f:42:b1 secure
linksys 00:06:25:7f:72:0f unsecured
Spoot 00:0f:66:a0:82:53 unsecured
coolawesomegals 00:09:5b:ed:79:a0 secure
2WIRE011 00:0d:72:32:ee:41 secure
NETGEAR 00:09:5b:da:70:bc unsecured
Lisa 00:09:5b:3d:65:5e secure
8315967210 00:0f:66:38:8b:f6 unsecured
main 00:0d:3a:27:a3:75 secure
linksys 00:0c:41:f6:0e:e5 unsecured
Chillaxin 00:0f:66:9a:f1:51 secure
00:0f:66:41:78:08 secure
00:09:5b:f9:d9:76 unsecured
linksys 00:0f:66:aa:fc:81 unsecured
default 00:0d:88:8c:fb:d9 unsecured
linksys 00:04:5a:fd:0c:51 unsecured
linksys 00:0f:66:c2:55:4c unsecured
2WIRE049 00:0d:72:9d:0d:99 secure
linksys2 00:0f:66:d7:e6:da unsecured
NETGEAR 00:09:5b:de:d8:08 unsecured
WLAN 00:30:bd:c1:54:02 unsecured
00:0c:41:f6:0e:e2 secure
cdg1315 00:0d:88:bb:f3:fb secure
NETGEAR 00:09:5b:ea:1f:54 secure
linksys 00:06:25:e7:a6:cf unsecured
linksys 00:0f:66:0b:39:a8 unsecured
wireless 00:90:4b:37:52:ae unsecured
21P 00:0f:3d:40:9f:58 secure
Whizzer 00:09:5b:47:f6:38 secure
winder_g 00:0f:b5:11:09:c2 secure
heatherjackiecory 00:0f:66:aa:70:49 unsecured
men 00:09:5b:de:d8:02 secure
bandgirls 00:0f:66:cc:14:eb unsecured
2WIRE728 00:0d:72:38:b3:a9 secure
royal 00:0c:41:3d:8b:22 secure
Wireless 00:09:5b:2a:05:12 unsecured
linksys 00:0f:66:03:5a:f9 unsecured
NETGEAR 00:09:5b:9c:2e:d6 unsecured
Silent Dragon 00:09:5b:ed:ba:6a secure
2WIRE931 00:0d:72:90:15:01 secure
default 00:0f:3d:36:1c:8f unsecured
linksys 00:06:25:f2:03:93 unsecured
rchamilt 00:0f:66:bc:72:36 secure
00:40:96:46:65:d5 secure
2WIRE734 00:0d:72:66:78:f9 secure
2WIRE499 00:d0:9e:f3:0b:b9 secure
linksys 00:0c:41:b7:99:1e secure
NETGEAR 00:09:5b:d8:60:ca unsecured
linksys 00:0f:66:3d:32:a6 unsecured
linksys 00:0f:66:94:78:16 unsecured
kurts 00:06:25:f1:67:21 secure
Johanna Northcote 00:0d:93:89:20:77 secure
JEWEL1 00:0c:41:3c:e5:62 unsecured
00:40:96:49:26:00 secure
wireless 00:06:25:06:17:f0 unsecured
linksys 00:06:25:90:06:3b unsecured
NETGEAR 00:09:5b:d7:da:6c unsecured
linksys 00:0c:41:ba:10:14 unsecured
linksys 00:0c:41:f3:1e:96 unsecured
linksys 00:0c:41:8a:13:d4 unsecured
linksys 00:06:25:a4:aa:c2 unsecured
default 00:0f:3d:49:cb:f6 unsecured
dlink 00:0d:88:20:4d:c4 secure

The Beast 00:09:5b:ff:74:d2 unsecured
Tom's House 00:40:05:b8:56:77 secure
uberspots.net 00:06:25:b9:4e:41 unsecured
linksys 00:0f:66:21:9b:8b unsecured
2WIRE024 00:0d:72:56:60:21 unsecured
00:04:5a:2f:dd:41 secure
linksys 00:0f:66:b0:bb:76 secure
monkey 00:0c:41:cb:5e:5f secure
nking 00:04:5a:ee:ea:05 secure
2WIRE032 00:0d:72:8f:16:49 secure
linksys 00:06:25:66:59:d2 secure
default 00:80:c8:1d:98:19 unsecured
linksys 00:0f:66:9b:e8:7f unsecured
AirPort 00:02:2d:29:74:fe secure
NETGEAR 00:09:5b:72:3c:b8 unsecured
casacondo 00:0c:41:b3:97:f2 secure
default 00:0f:3d:3d:b2:7e unsecured
linksys 00:0c:41:45:0a:aa unsecured
1326GalleonWay#1 00:09:5b:fa:6d:d8 secure
richmitch 00:12:17:08:e2:bf secure
galleon 00:0f:66:3d:39:60 unsecured
NETGEAR 00:09:5b:ff:66:56 unsecured
linksys 00:06:25:f4:6b:03 unsecured
00:06:25:5b:1b:b1 secure
linksys 00:0f:66:aa:c3:83 unsecured
default 00:0d:88:20:4e:22 unsecured
linksys 00:0f:66:3d:39:5a unsecured
linksys 00:0c:41:41:0b:fc unsecured
fosgood 00:09:5b:9b:29:d0 unsecured
linksys 00:06:25:76:c1:db unsecured
Oceanaire 00:06:25:fb:18:3c secure
Tabone 00:0c:41:18:99:e8 secure
Apple Network 007173 00:11:24:00:71:73 unsecured
ROBH 00:02:2d:c4:47:ba unsecured
Viola's Network 00:0a:95:f4:24:f8 secure
linksys 00:0c:41:49:ef:04 secure
linksys 00:0c:41:f6:0e:dc unsecured
no. 37 00:0f:66:b8:83:dc secure
Booker 00:09:5b:9f:4a:4e unsecured
fluffy 00:0c:41:c0:4e:85 unsecured
default 00:0d:88:25:34:55 unsecured
Wireless 00:09:5b:3d:64:f0 unsecured
Lynch 00:09:5b:d9:13:b8 unsecured
Pleasanton 00:0c:41:9c:05:a7 unsecured
J's Airport 00:0d:93:8b:98:8d secure

KeepOff 00:50:f2:ce:63:e0 secure
2WIRE763 00:0d:72:8f:25:59 secure
Leonardo 00:0f:66:8c:35:d3 unsecured
mariana 00:0f:66:ca:e8:ed unsecured
WLAN 00:01:24:f0:3e:fc unsecured
belkin54g 00:11:50:0d:c4:fd unsecured
27H 00:09:5b:6e:a4:9c secure
linksys 00:0c:41:3c:bf:5e unsecured
IHH 00:40:05:ca:35:a2 secure
NETGEAR 00:09:5b:9d:4c:04 unsecured
Utopia 00:09:5b:9f:7a:1e secure
skyriver 72:fe:e6:7f:5a:d3 unsecured
WNR2004 00:30:ab:24:8c:1a secure
2WIRE133 00:d0:9e:c2:84:01 secure

00:30:bd:95:7b:75 secure
Harvey 00:0f:66:a7:8d:a3 secure
linksys 00:0c:41:a1:50:70 unsecured
scott 00:0c:41:41:99:b8 unsecured
PimpLan 00:30:ab:16:b6:3a secure
2WIRE299 00:d0:9e:e7:dd:31 secure
promark 00:0f:66:41:78:0b unsecured
00:40:96:49:3e:17 secure
linksys 00:0f:66:c3:b6:b9 unsecured
royaloak 00:0f:66:28:d5:d1 unsecured
royaloak 00:02:2d:aa:4b:17 unsecured
linksys 00:0c:41:71:85:70 unsecured
linksys 00:0f:66:0b:07:74 unsecured
2WIRE553 00:0d:72:91:ed:a1 secure
TheSyndicate 00:09:5b:aa:a4:a2 unsecured
kk 00:0f:34:42:92:50 unsecured
kk 00:0f:34:42:90:f0 unsecured
kk 00:0f:34:42:91:a0 unsecured
2WIRE422 00:0d:72:93:3d:39 secure
2WIRE510 00:0d:72:b3:28:a1 secure
linksys 00:0f:66:0b:96:ed unsecured
linksys 00:0c:41:47:d0:88 unsecured
linksys 00:0f:66:b1:d8:01 unsecured
2WIRE058 00:0d:72:3e:7c:79 unsecured
atomic designs 00:0c:41:4b:5b:9a unsecured
JJ 00:0f:3d:49:eb:4e secure
00:06:25:66:82:64 unsecured
Romero 00:12:17:02:da:5d unsecured
default 00:0d:88:2c:2b:e1 unsecured
Nicks Shack 00:06:f4:06:b7:36 secure
Neal 00:30:bd:c8:f4:78 unsecured
Ryan 00:0f:66:8e:ae:51 secure
slocrusade 00:09:5b:fb:8e:34 unsecured
NETGEAR 00:09:5b:ea:4c:0a unsecured
2WIRE048 00:0d:72:7e:bf:19 secure
linksys 00:06:25:e5:fa:09 unsecured
Slack 00:0f:66:cb:03:39 secure
linksys 00:0c:41:45:0a:68 unsecured
linksys 00:0c:41:71:b3:b0 unsecured
2WIRE202 00:d0:9e:d2:2b:e1 secure
NETGEAR 00:09:5b:ca:fe:e6 unsecured
2WIRE479 00:0d:72:97:a9:81 secure
Jeff 00:30:bd:93:7f:35 unsecured
linksys 00:0c:41:c6:83:af unsecured
default 00:05:5d:ec:90:6e unsecured
2WIRE625 00:0d:72:9b:3b:29 secure
linksysA 00:0f:66:c2:20:12 unsecured
default 00:40:05:b4:7d:f7 unsecured
2WIRE630 00:d0:9e:f1:ff:21 secure
default 00:80:c8:1b:3f:d5 unsecured
linksys 00:0f:66:95:b3:53 unsecured
NETGEAR 00:09:5b:b1:bf:ca unsecured
2WIRE471 00:0d:72:9a:1b:49 secure
2WIRE514 00:d0:9e:d2:4e:51 secure
princess 00:0f:66:b8:83:d0 secure
default 00:0d:88:94:50:bd secure
default 00:0d:88:c2:af:71 unsecured
linksys 00:0f:66:ca:df:19 unsecured
2WIRE752 00:0d:72:64:ce:41 secure
hathway 00:0f:66:d7:bc:6e unsecured
linksys 00:0c:41:41:0c:06 unsecured
AHK 00:0f:66:21:51:f7 secure
SigEpNet 00:06:25:24:c1:e7 unsecured
linksys 00:0c:41:45:2b:e0 unsecured
linksys 00:0c:41:43:8e:10 unsecured
linksys 00:0c:41:41:15:48 unsecured
Efird 00:0c:e5:4a:1b:81 unsecured
Buenotastic 00:00:d1:23:41:6c unsecured
KP4LIFE 00:0f:66:d7:bc:53 secure
mweaver 00:06:25:0e:a8:bb unsecured
2WIRE592 00:d0:9e:f3:f3:f1 secure
NETGEAR 00:09:5b:af:4d:aa unsecured
2WIRE765 00:0d:72:9a:8e:21 secure
browncar wireless 00:0f:66:8f:97:68 unsecured
Team Munson 00:0f:66:0c:64:ee secure
PUZOL 00:0f:3d:51:62:54 secure
2WIRE299 00:0d:72:99:69:f1 secure
linksys 00:0f:66:cc:bd:2d unsecured
default 00:0f:3d:5e:a5:f4 unsecured

SHOWTIME 00:0c:41:66:cf:bc secure
linksys 00:12:17:0e:51:d3 unsecured
linksys 00:06:25:b6:32:ab unsecured
Apple Network 82d1b9 00:0d:93:82:d1:b9 unsecured
calpolylink 00:04:5a:ed:4b:43 secure
linksys 00:12:17:0b:5d:d2 unsecured
linksys 00:0f:66:56:51:3b unsecured
C4 00:40:05:b4:7a:07 secure
linksys 00:06:25:6d:ea:b7 unsecured
linksys 00:0f:66:c2:54:c8 unsecured
default 00:80:c8:14:4d:25 unsecured
Get your own Bandwidth 00:0f:66:d0:e4:ee secure
mweaver 00:06:25:0e:95:25 unsecured
SBE 00:09:5b:6f:c4:92 secure
SBE11-2 00:40:05:b6:38:39 secure
gunit 00:06:25:75:e2:eb unsecured
neatness 00:12:17:0b:e5:4a secure
Wireless 00:09:5b:54:d7:20 unsecured
NETGEAR 00:09:5b:50:80:60 unsecured
NETGEAR 00:09:5b:50:50:4c unsecured
home32 00:06:25:87:5e:e5 unsecured
SBE11 00:0d:88:81:af:18 secure
linksys 00:0f:66:a9:f2:b7 unsecured
EBS 00:0d:88:8d:41:d5 secure
MSHOME 00:50:f2:cb:ef:5e unsecured
linksys 00:06:25:f1:91:c0 unsecured
NETGEAR 00:09:5b:cd:5a:2c unsecured
WeLikeDogsButILikeCats 00:0f:66:39:67:9e secure
linksys 00:0f:66:01:6d:97 unsecured
default 00:0d:88:87:01:57 unsecured
Apt. #33 00:30:ab:1f:a8:a2 unsecured
PimpHotel 00:c0:49:e5:19:6c secure
linksys 00:0f:66:4e:19:93 unsecured
linksys 00:0f:66:56:c8:33 unsecured
00:0f:66:c4:2d:2a unsecured
ninor 00:06:25:62:e2:0e secure
default 00:0f:3d:5a:bd:c0 unsecured
weed 00:0f:66:47:f8:28 unsecured
cisco 00:0c:41:ac:8a:08 secure
linksys 00:0f:66:9a:f0:25 unsecured
2WIRE808 00:0d:72:9c:f5:21 secure
Virus 00:40:05:5b:8f:df secure
linksys 00:0c:41:43:8d:94 unsecured
SpeedStream 00:c0:02:cc:ec:70 unsecured
2WIRE973 00:d0:9e:ef:34:51 secure
Crazyhouse 00:04:e2:b6:9a:08 secure
th7 00:0f:66:aa:7f:b1 unsecured
2WIRE998 00:0d:72:5a:a5:91 secure
NETGEAR 00:09:5b:c3:6c:4e secure
default 00:0f:3d:51:5f:c2 secure
linksys 00:0f:66:c6:13:06 unsecured
108 00:40:05:24:4f:db secure
linksys 00:0c:41:49:18:e1 unsecured
Chops 00:0f:66:3e:d7:03 secure
windent 00:80:c8:aa:c3:59 unsecured
default 00:50:18:0a:6d:44 unsecured
linksys 00:0f:66:35:80:86 unsecured
00:0f:3d:4e:f4:ee unsecured
katamanda 00:09:5b:dd:41:9c secure
NETGEAR 00:09:5b:fa:8c:14 unsecured
GODZILLA 00:0f:66:56:c8:27 secure
2WIRE322 00:0d:72:9b:55:01 unsecured
car ramrod 00:40:05:b7:f3:cf unsecured
2WIRE787 00:d0:9e:d2:f0:a1 secure
byrons 00:06:25:a3:e1:e4 unsecured

2WIRE213 00:0d:72:65:21:79 secure
40CASA 00:12:17:12:c7:a8 secure
2WIRE822 00:0d:72:84:cd:09 secure
linksys 00:0f:66:2b:05:31 unsecured
cedarcreekhoes 00:90:4b:37:7a:da unsecured
default 00:0d:88:b7:04:ba unsecured
linksys 00:0f:66:22:67:5b unsecured
default 00:80:c8:b7:a7:54 secure
linksys 00:0f:66:94:6a:ce unsecured
WLAN 00:01:24:f2:ee:bf unsecured
NETGEAR 00:09:5b:4e:e0:62 unsecured
2WIRE232 00:d0:9e:ca:08:a1 secure
2WIRE646 00:0d:72:85:c0:61 secure
default 00:0d:88:88:35:7d secure
BigPimpin' 00:05:5d:fb:01:a2 unsecured
NETGEAR 00:09:5b:4d:65:4e unsecured
linksys 00:0f:66:aa:c5:79 unsecured
linksys 00:0f:66:c3:1e:ca unsecured
jackie 00:06:25:fa:82:63 secure
2WIRE874 00:d0:9e:f4:3f:a9 secure
linksys 00:0c:41:71:b2:9a secure
linksys1 00:0c:41:43:8e:16 unsecured
brittany 00:0d:88:94:50:a9 unsecured
default 00:0f:3d:43:9d:98 unsecured
2WIRE226 00:d0:9e:cb:a6:51 secure
home 00:0c:41:72:79:5e unsecured
belkin54g 00:11:50:05:5d:09 unsecured
linksys 00:0f:66:23:75:11 unsecured
OhioStateFan 00:09:5b:da:40:6a secure
00:0f:66:92:29:a4 unsecured
Stenner55O 00:12:17:0b:5d:fc unsecured
belkin54g 00:30:bd:fb:9d:53 unsecured
Heaven55D 00:50:18:06:9e:9a secure
NETGEAR 00:09:5b:9d:b4:0a unsecured
upskirt_honeyz 00:0f:66:cb:03:1b unsecured
McGov 00:0f:66:c3:b6:c5 secure
2WIRE825 00:0d:72:6c:2d:e1 secure
DX 00:0f:3d:61:a8:ac unsecured
amandaandallison 00:0f:66:c3:ba:49 unsecured
ChadMatt 00:06:25:be:8a:d3 unsecured
00:09:5b:3d:93:a4 secure
Chad 00:0f:66:9a:f1:11 unsecured
pimphouse 00:0f:66:42:cb:71 secure
2WIRE962 00:d0:9e:9b:48:f1 secure
NETGEAR 00:09:5b:fa:30:9e unsecured
NETGEAR 00:09:5b:53:03:96 secure
linksys 00:0f:66:b1:a7:53 unsecured
slodudes 00:0c:41:4f:c9:f4 secure
stenner 00:12:17:0e:a4:50 secure
Adam1 00:0f:66:d8:14:16 unsecured
default 00:0d:88:8d:47:71 unsecured
00:02:2d:3c:e4:34 unsecured
wireless 00:0c:41:6f:b8:dc unsecured
linksys 00:0c:41:45:2b:78 unsecured
NETGEAR 00:09:5b:e5:50:ca unsecured
I_want_some_crack 00:0f:66:35:da:10 secure
Kris 00:0f:3d:3f:fd:b4 secure
00:0f:66:01:bc:1b unsecured
linksys 00:0c:41:4e:6f:b0 unsecured
NETGEAR 00:09:5b:51:85:be unsecured
jdeleuw 00:0c:41:71:76:a6 secure
Murray - Common 00:02:2d:b4:b6:88 unsecured
Murray St. 00:06:25:eb:e9:22 unsecured
wireless 00:90:4b:36:d2:56 unsecured
nicolesux 00:09:5b:fb:a8:b8 unsecured
Jessica 00:0c:41:3c:a9:14 unsecured
aptc 00:04:5a:2e:34:d5 secure
Jason 00:12:17:0b:5d:f3 secure
linksys3 00:12:17:09:70:d0 secure
linksys 00:0c:41:47:9a:fa unsecured
Homer 00:0f:66:d7:e6:56 unsecured
521 Hathway 00:06:25:db:54:75 unsecured
00:0f:66:c6:13:03 unsecured
default 00:0d:88:2b:ba:01 unsecured

walnut 00:0f:66:56:c8:1d unsecured
SpeedStream 00:c0:02:cf:29:fe unsecured
default 00:40:05:5c:6c:39 unsecured
linksys 00:06:25:f6:24:fa unsecured
Boar Tusk 00:04:5a:0f:21:70 unsecured
linksys 00:0f:66:ca:e8:eb unsecured
default 00:0f:3d:49:d6:c4 unsecured
cockmonger 00:0c:41:a1:30:80 unsecured
linksys 00:0c:41:43:8d:90 unsecured
wireless 00:90:4b:31:88:f6 unsecured
Dude 00:0d:88:a1:13:ef secure
linksys 00:0c:41:41:0b:e8 unsecured
linksys 00:0f:66:c3:61:06 unsecured
2WIRE478 00:0d:72:67:bd:f9 secure
SLOAMB 00:0f:66:4f:b0:6b unsecured
ANY 00:04:e2:30:1a:3a unsecured
00:0d:72:63:fd:21 secure
SantaRosa 00:40:05:ba:76:b7 unsecured
linksys 00:0f:66:c3:ba:10 secure
KPTA 00:06:25:0e:cc:a6 secure
KPTG 00:0c:41:17:2c:ed secure
KPTA 00:06:25:1e:fe:af secure
linksys 00:0f:66:0b:07:4d unsecured
KPTG 00:0c:41:17:29:e8 secure
SANTA ROSA HOME 00:0d:88:40:fc:19 secure
greenhouse 00:0f:66:ca:e8:ef unsecured
00:0f:66:8d:ed:8b secure
LBR 00:0f:66:56:69:f7 unsecured
salientarmy 00:0f:66:52:d8:fc unsecured
default 00:40:05:b1:6a:bf unsecured
Red Eye Express 00:11:24:00:ef:19 secure
linksys 00:06:25:7d:b5:f3 unsecured
linksys 00:0f:66:9a:f0:0f secure
linksys 00:12:17:1a:ef:be unsecured
GOD 00:0c:41:36:a5:5b unsecured
slpbeauty 00:0f:66:47:65:76 secure
NETGEAR 00:09:5b:6a:28:d6 unsecured
linksys 00:12:17:0c:37:25 unsecured
fuckoff 00:0d:72:2c:55:09 secure
CaseyInternet 00:09:5b:24:80:d2 unsecured
default 00:0d:88:c2:94:13 unsecured
intrigue 00:06:25:48:d8:0b unsecured
linksys 00:06:25:77:62:c9 unsecured
wobbly 00:0f:66:2d:cf:f7 unsecured
jk1996 00:12:17:2b:e1:0a unsecured
linksys 00:0c:41:71:b2:98 unsecured
mywireless 00:0f:66:c2:09:0c unsecured
2WIRE937 00:d0:9e:be:7d:b1 secure
goaway 00:80:c8:b0:cc:2a secure
2WIRE373 00:0d:72:6e:a1:31 secure
Mishka 00:02:2d:29:71:0d unsecured
slod linksys 00:0f:66:30:26:41 unsecured
NETGEAR 00:09:5b:ea:33:da unsecured
2WIRE998 00:0d:72:67:31:61 secure
newjamiaca 00:09:5b:c2:7a:a6 unsecured
MSHOME 00:0d:3a:27:52:4f unsecured
2dayULook 00:0f:66:c3:b6:8f unsecured
linksys 00:0f:66:e3:8e:8c secure
STUD FARM 00:09:5b:da:70:f4 secure
00:d0:9e:dc:57:b1 unsecured
MorningStar 00:09:5b:ad:e9:38 unsecured
2WIRE365 00:0d:72:9a:4c:71 secure
WLAN 00:30:bd:c4:91:e2 unsecured
popcorn333 00:0c:41:cc:92:e5 unsecured
lisa 00:0f:66:46:7a:7a secure
4SLOGuys 00:09:5b:c9:3e:32 secure
default 00:0f:3d:5b:86:1e unsecured
2WIRE114 00:0d:72:34:20:d9 secure
1446Lizzie 00:50:18:04:d7:aa secure
linksys 00:0f:66:22:b0:77 unsecured
2WIRE136 00:0d:72:91:e3:f1 secure
linksys 00:0f:66:2c:7c:a6 unsecured
peach 00:e0:b8:6a:f4:46 unsecured
NETGEAR 00:09:5b:86:3b:ae unsecured
alhg 00:0d:88:ba:f1:c7 unsecured
home 00:90:4b:36:91:da unsecured
linksys 00:06:25:77:01:03 unsecured
linksys 00:06:25:a1:e8:6e unsecured
2WIRE729 00:d0:9e:db:8e:31 secure
Brigham Wireless 00:09:5b:35:b5:0a unsecured
ilovejudy 00:06:25:59:bb:c8 secure
2WIRE182 00:0d:72:a1:b2:e9 secure
linksys 00:06:25:ff:61:04 unsecured
sparky 00:09:5b:ed:9d:86 unsecured
linksys 00:0c:41:79:74:f0 unsecured
00:0d:88:97:da:06 secure
The Strip 00:06:25:f6:27:12 unsecured
linksys 00:06:25:fa:8f:6c unsecured
Precision 00:50:f2:74:7a:44 secure
linksys 00:0f:66:94:76:d0 unsecured
2WIRE006 00:02:2d:89:cd:f8 secure
1512 00:0f:66:41:85:3d unsecured
linksys 00:12:17:0b:5d:ed unsecured
default 00:0d:88:1f:f6:f2 unsecured
LittleYellowHouse 00:0c:41:7f:fe:92 unsecured
2WIRE098 00:0d:72:91:cb:01 secure
NETGEAR 00:09:5b:51:ab:b2 unsecured
Ihatecharter 00:06:25:86:67:ad unsecured
linksys 00:0f:66:23:a6:af unsecured
default 00:e0:98:4f:bb:da unsecured
sarah net 00:0f:66:bf:3a:9a unsecured
Nerd Central 00:0f:66:aa:c4:af secure
SarahNet 00:12:17:01:9d:b9 secure
! eb&j 00:0f:66:9a:f2:4f unsecured
IEEE 802.11 LAN 00:90:96:23:7e:80 unsecured
leber 00:0c:41:76:c5:3c unsecured
linksys 00:0f:66:56:69:fb unsecured
linksys-g 00:06:25:b2:a2:8b unsecured
linksys 00:0f:66:40:7e:18 unsecured
linksys 00:04:5a:2e:0a:9d unsecured
Base Station 00:0d:93:83:c8:8e secure
go-slo 00:06:25:ec:08:d6 secure
Base Station 00:11:24:00:df:f5 secure
Buck Futter 00:09:5b:3c:02:b0 secure
feotips 00:09:5b:4e:8c:7c secure
default 00:0f:3d:49:d3:56 secure
linksys 00:0c:41:cc:69:89 secure
linksys 00:0f:66:c1:d0:e6 unsecured
linksys 00:0f:66:ca:df:05 unsecured
2038 00:0f:66:8c:51:49 unsecured
Wireless 00:09:5b:54:ab:27 unsecured
BIG 00:09:5b:4e:66:f6 unsecured
Apple Network 00:11:24:00:f2:bf unsecured
wireless 00:90:4b:39:77:84 unsecured
wireless 00:90:4b:39:19:14 unsecured
Broad Street 00:0f:66:4c:38:de unsecured
Wireless 00:0f:66:9a:f0:b9 unsecured
2WIRE139 00:0d:72:32:97:29 secure
linksys 00:0c:41:6f:77:9c unsecured
2WIRE389 00:0d:72:5e:0a:e9 secure
Gibson 00:11:24:00:e6:e1 secure
linksys 00:0f:66:38:71:9e unsecured
linksys 00:0c:41:c8:45:a5 unsecured
WLAN 00:01:24:f4:27:3c unsecured
Wireless 00:09:5b:47:e5:74 unsecured
linksys 00:0f:66:be:fc:ce unsecured
bambam 00:0f:66:01:6d:85 unsecured
Wireless 00:30:ab:1c:f4:b4 unsecured
2WIRE227 00:0d:72:99:70:f1 secure
Gin's airport 00:30:65:0a:44:f5 secure

SushiMasters 00:09:5b:52:23:30 unsecured
2WIRE 00:d0:9e:f6:b4:59 unsecured
slo727 00:06:25:fa:ab:40 unsecured
sophie 00:0f:66:2f:aa:d1 unsecured
riderlink 00:06:25:77:23:ff unsecured
2WIRE749 00:d0:9e:ac:44:01 secure
bauer 00:0c:41:ca:89:71 secure
00:0c:41:79:d4:8a unsecured
explodingvarmit 00:0f:3d:00:61:a5 secure
00:0f:66:22:fb:d5 unsecured
NETGEAR 00:09:5b:70:0d:70 unsecured
geeksquad396 00:0f:66:8d:c4:d5 secure
2WIRE625 00:0d:72:92:58:79 secure
jmrouter 00:0c:41:3d:8b:2e secure
thecasa 00:0f:66:9c:ad:86 secure
linksys 00:0f:66:02:1b:79 unsecured
00:0f:66:c4:33:21 unsecured
00:09:5b:fa:fb:fa secure
BC Home 00:0d:88:a0:f4:7b secure
NETGEAR 00:09:5b:d8:be:a2 unsecured
linksys 00:0f:66:74:f3:91 unsecured
linksys 00:0f:66:35:ee:d4 unsecured
linksys 00:0f:66:db:3c:83 unsecured
linksys 00:0f:66:2f:f3:93 unsecured
RandJandSandS 00:0c:41:c0:c8:33 unsecured
2WIRE470 00:d0:9e:ac:38:d1 secure
lynn 00:0f:66:02:9b:a4 unsecured
2WIRE783 00:d0:9e:a8:a9:71 secure
NETGEAR 00:09:5b:ff:78:e2 unsecured
Gateway 00:e0:b8:6a:e2:bc secure
jeffoberti 00:40:05:b7:e7:db secure
jan 00:06:25:89:09:69 unsecured
linksys 00:04:5a:e4:e2:49 unsecured
Honor 00:12:17:0b:9f:33 secure
Fire Inc. 00:0f:66:9f:24:07 secure
38 00:0f:66:9a:f0:9d unsecured
00:0f:66:21:b5:ef unsecured
NETGEAR 00:09:5b:4d:cb:fc unsecured
linksys 00:0f:66:3c:f2:18 secure
linksysPr b6:38:b5:c7:bc:42 secure
NETGEAR 00:09:5b:c8:a6:98 unsecured
NETGEAR 00:09:5b:cf:6a:38 unsecured
00:04:5a:fd:c3:bf unsecured
linksys 00:0f:66:47:69:c6 unsecured
2WIRE004 00:d0:9e:f2:67:09 secure
expohouse 00:09:5b:ea:63:26 secure
kelly 00:0c:41:73:5a:46 unsecured
hub 00:04:5a:26:f7:cb unsecured
NielsenNet 00:0d:93:8b:6e:26 secure
BLUE 00:0d:88:97:aa:8c secure
linksys 00:06:25:77:86:fd unsecured
MusicBox 00:0c:41:3d:8b:38 unsecured
wireless 00:90:4b:33:68:90 unsecured
balls 00:0f:66:ad:44:b3 unsecured
woodbridge 00:0c:41:8a:2b:ac unsecured
linksys 00:0f:66:89:ff:be unsecured
linksys 00:06:25:62:f8:fc unsecured
GnomeNet 00:0c:41:67:ec:17 secure
fez 00:0f:66:aa:72:5d secure
Wireless0wnage 00:09:5b:34:b2:71 unsecured
sofie2000 00:30:bd:93:5e:3d unsecured
TheFury 00:0f:66:bb:00:78 secure
default 00:80:c8:03:86:28 secure
2WIRE022 00:0d:72:13:9f:81 secure
2WIRE928 00:0d:72:61:33:69 unsecured
NETGEAR 00:09:5b:aa:8f:5a unsecured
HALENET 00:06:25:3c:be:f6 secure
tascommnet 00:02:2d:c4:4b:4d unsecured
00:40:96:40:6b:39 secure
raytheon2 00:02:2d:c4:4b:3a unsecured
WLAN 00:30:bd:c2:63:c4 secure
ssid123 00:0f:3d:37:67:2e unsecured
hautespot 00:02:6f:05:5e:01 unsecured
hautespot 00:02:6f:03:89:89 unsecured
parable 00:09:5b:36:11:ce unsecured
tmobile 00:09:e8:b4:ff:a1 unsecured
metro 00:0c:41:f7:d5:ee unsecured
BNDEMO 00:a0:f8:3b:cf:be secure
BNDEMO 00:a0:f8:41:ef:56 secure
FreedomLink 00:0f:8f:51:09:b0 unsecured
FreedomLink 00:0f:34:48:2f:40 unsecured
BNDEMO 00:a0:f8:3b:cf:ba secure
Wireless 00:30:ab:16:20:27 secure
2WIRE521 00:0d:72:90:c2:59 secure
NETGEAR 00:09:5b:da:36:16 unsecured
lockshop 00:0c:41:c0:66:55 secure
00:06:25:64:96:1c unsecured
fentanyl 00:0f:66:56:63:89 secure
linksys 00:0c:41:8a:55:f2 unsecured
linksys 00:0c:41:47:9a:ec unsecured
00:0c:41:b1:97:72 unsecured
GlobalSuiteWireless 00:a0:f8:ae:99:68 unsecured
GlobalSuiteWireless 00:a0:f8:af:9c:50 unsecured
linksys 00:06:25:24:b0:9a unsecured
villa1670motel 00:06:25:da:34:a6 secure
linksys 00:0f:66:24:30:bd unsecured
linksys 00:0f:66:24:30:c7 unsecured
skyriver 00:0d:08:06:21:16 unsecured
skyriver 00:0d:08:06:1c:21 unsecured
grand 00:0f:66:56:79:3f unsecured
jennandchels 00:0f:66:22:7d:c1 unsecured
Wireless 00:09:5b:3f:41:3d unsecured
linksys 00:06:25:7d:91:1f unsecured
linksys 00:0f:66:c2:09:04 unsecured
2WIRE019 00:0d:72:b9:9c:29 secure
2WIRE865 00:02:2d:a4:58:46 secure
Cue_ball 00:09:5b:aa:28:06 unsecured
WLAN 00:30:bd:c2:76:32 unsecured
CCMAG 00:09:5b:dd:b8:38 secure
craziesilly 00:40:05:56:79:05 secure
Bio nerds rule 00:0f:66:9e:1c:37 unsecured
default 00:0d:88:3e:8f:69 unsecured
cockmonger 00:0c:41:6f:b8:c4 unsecured
bwsomersetinn 00:0d:88:ba:72:b8 secure
Morgan 00:0f:66:2a:b8:21 secure
skyriver 00:0d:08:06:1c:17 unsecured
2661lasgallinas 00:0f:66:43:4d:64 unsecured
linksys 00:0f:66:9f:c3:c9 unsecured
KRL 00:09:5b:dd:82:c6 secure
morpheus 00:09:5b:86:c3:0e unsecured
2WIRE203 00:0d:72:97:fc:d1 secure
Buttercup 00:06:25:d9:4b:55 secure
linksys 00:06:25:78:44:f5 unsecured
linksys 00:06:25:55:8a:06 unsecured
Lopez 00:50:18:07:70:aa secure
linksys 00:0c:41:6f:a6:c6 unsecured
NETGEAR 00:09:5b:da:46:f4 unsecured
Patrick 00:0d:93:80:fc:9c secure
2WIRE880 00:0d:72:9c:f9:49 secure
Wireless 00:09:5b:29:4a:25 unsecured
linksys 00:06:25:24:f2:a6 unsecured
linksys 00:0f:66:9f:c3:d7 unsecured
linksys 00:0f:66:39:16:d4 unsecured
linksys 00:0c:41:49:fe:66 unsecured
test 00:0f:66:00:62:19 unsecured
linksys 00:0c:41:41:3b:5e unsecured
Wireless 00:30:ab:1d:c4:39 unsecured
Orange_CalPoly 00:0c:41:cb:c9:a2 unsecured
NETGEAR 00:09:5b:dd:82:3e unsecured
1214 Bond 00:06:25:7d:ef:ad unsecured

231 00:06:25:e6:90:6d unsecured
linksys 00:0f:66:40:37:88 unsecured
default 00:0d:88:40:ef:03 unsecured
NETGEAR 00:09:5b:fa:31:0c unsecured
00:11:50:09:cf:ab secure
linksys 00:02:dd:85:2e:14 unsecured
NETGEAR 00:09:5b:9f:1a:68 unsecured
joe 00:09:5b:fa:6d:e0 unsecured
aptA 00:0f:66:aa:72:8d unsecured
linksys 00:0c:41:42:f0:ce unsecured
Simon 00:06:25:f6:06:28 unsecured
glow worm 00:0f:3d:37:f3:f0 secure
dawn 00:0f:66:a9:f6:8f secure
2WIRE218 00:0d:72:24:d5:99 secure
home 00:09:5b:c5:78:de secure
sseleriw 00:40:05:5d:1e:b5 unsecured
NETGEAR 00:09:5b:51:8a:32 unsecured
linksys 00:0f:66:9a:f0:f5 unsecured
Slack 00:0d:72:9b:28:c9 secure
default 00:0f:3d:49:a3:ea unsecured
linksys 00:0c:41:b1:1a:8c unsecured
linksys 00:0f:66:56:51:33 unsecured
2WIRE784 00:0d:72:90:33:09 secure
linksys 00:06:25:e7:d1:51 unsecured
linksys 00:06:25:86:f5:9b unsecured
Arizona 00:06:25:90:04:8d unsecured
linksys 00:0c:41:76:43:fe unsecured
Apple Network 088e03 00:11:24:08:8e:03 secure
2WIRE163 00:0d:72:99:a6:01 secure
linksys 00:0f:66:bd:70:0a unsecured
linksys 00:0f:66:aa:72:7d unsecured
MSHOME 4a:bc:78:4a:7e:89 unsecured
00:0f:66:cc:e2:08 unsecured
MustangWireless 00:40:96:45:ef:4e unsecured
linksys 00:0c:41:71:15:66 unsecured

WORKS CITED

[2Wire03] 2Wire, Inc. HomePortal Installation and Support Guide. 2003.

[Bradley03] "Drive-By Net User Targets Kid Porn; Cops: 'War Driving' Grows." Toronto Sun 22 November, 2003: 4

[Cobbs04] Cobbs, Chris. "Is Open Access an Invitation?". February 27, 2003. The Mercury News. October 7, 2004 <http://www.mercurynews.com/mld/mercurynews/business/5274558.htm>.

[Code502] "CA Codes (pen. 484-502.9)." Official California Legislative Information. November 21, 2004 <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=484-502.9>.

[Code601] "CA codes (pen. 594-625c)." Official California Legislative Information. November 21, 2004 <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=pen&group=00001-01000&file=594-625c>.

[Dvorak04] Dvorak, John C. "The Looming Legal Threat to Wi-Fi." PC Magazine 4 May 2004: 63.

[Everett04] Everett, Cath. "Special Report; Wireless: The Importance of Securing Your Network." Computing 29 April 2004: 25.

[Johnson04] Johnson, Deborah G. Computer Ethics. Saddle River, New Jersey: Prentice Hall, 2002.

[Marr04] Marr, John. "Drive-by hackers". Sunday Mail 13, June 2004: 111.

[Poulsen04] Poulsen, Kevin. Wardriver pleads guilty in Lowes WiFi hacks. June 4, 2004. SecurityFocus. October 7, 2004 <http://www.securityfocus.com/news/8835>.

[Rist04] Rist, Oliver. "Enterprise Windows: Legalities and Wardriving." InfoWorld Daily News. September 17, 2004 <http://www.infoworld.com/article/04/09/17/38enterwin_1.html>.

[SBC04] "SBC Yahoo! DSL Home Networking/Office Gateway Special Offer – CA." SBC Communications. November 21, 2004 <http://owl.english.purdue.edu/handouts/research/r_mla.html>.

[SCOE] "Software Engineering Code of Ethics and Professional Practice." IEEE Computer Society. November 21, 2004 <http://www.computer.org/tab/seprof/code.htm>

[Wade02] Wade, Carole, and Carol Tavris. Introduction to Psychology. Saddle River, New Jersey: Prentice Hall, 2002.

[wiki04] IEEE 802.11. October 5, 2004. Wikipedia. October 7, 2004. <http://en.wikipedia.org/wiki/IEEE_802.11>.