Getting Started with Free Wireless Networks

NYCwireless' guide to setting up a node for public access

Table of Contents

==========

1. Introduction.

This is a simple guide for users who want to set up a Public Node and add it to the NYCwireless Node map. This guide assumes you are using Microsoft Windows unless specified. Use the guide and help grow the NYCwireless network.

1.1 NYCwireless Mission Statement (v.1.0.1)

· Provide Free Public Wireless Internet Service - NYCwireless provides free wireless Internet service using wireless technology to mobile users in public spaces throughout the New York City metropolitan area. These public spaces include parks, coffee shops, and building lobbies. NYCwireless intends to work with public and other nonprofit organizations to bring broadband wireless Internet to under-served communities.

· Provide a Forum for Wireless Networking - NYCwireless provides a forum for technical and non-technical issues of wireless Internet technology especially for those interested in building wireless community networks. Through online discussion groups, workshops and meetings, NYCwireless provides information about wireless internet technology to individuals wishing to provide their own wireless access points as well as developers of wireless technology. The organization seeks to promote the development of wireless software applications based on the open source model. The organization also seeks to promote the research, development, and use of the next generation of mobile ad-hoc wireless mesh networks.

· Advocate of Wireless Community Networking - NYCwireless serves as an advocacy group for wireless community networking. Through a business outreach program, communication with the press and participation in conferences, NYCwireless seeks to educate the general public and businesses about the benefits of wireless community networking. NYCwireless seeks to utilize existing wireless technologies and incorporate evolving wireless technologies as they become available.

· Emergency Communications Network - NYCwireless seeks to work with city, state, federal, and other authorities and organizations to build an Emergency Communications IP network in conjunction with the existing NYCwireless networks.

1.2 Resources guide.

There are many resources available on the web that deal with Access Point reviews, hardware modification, antenna choice, and many other topics related to operating your public node.

Practically Networked (http://www.practicallynetworked.com) and Small Net Builder (http://www.smallnetbuilder.com) have many thorough and comprehensive reviews of both Access points and various wireless NICs.

The Personal Telco Project has a very extensive list of topics that deal with wireless networking. Their website is http://www.personaltelco.net.

NoCat - a group based in Sonoma County, California - maintains a FAQ. http://nocat.net/faq.txt

2. Choosing an ISP.

If you have Business-Class Internet service you should have no issues with allowing outside users to share your network wirelessly. As a general rule, Business Class contracts do not specifically restrict any forms of usage within the legal realm. However be sure to check the Acceptable Usage Policy (AUP) or Terms of Service (TOS) agreement with your provider.

When you use Residential-Class Internet service, please check the TOS or AUP of your provider to see whether they allow sharing with others. The Personal Telco Website maintains a list of ISP policies with regard to sharing your connection wirelessly (http://www.personaltelco.net/index.cgi/IspWirelessPolicies).

For the New York City area NYCwireless recommends using: Bway.Net (http://www.bway.net), Cloud9.Net (http://www.cloud9.net), and Ace DSL (http://www.acedsl.com).

3. Choosing an Access Point.

The Access Point functions as the root of your wireless network. It can be a Linux box running networking services, or it can be an out-of-the-box router, complete with firewall and print sharing capabilities. As a general rule, you can use any access point that uses the Wi-Fi standard and set it up for public use.

3.1 Tried and True access points by many users.

Many users have had success with the Apple Airport Base Station and Orinoco RG-1000. They are fairly simple to configure, and with a bit of tinkering can be modified to allow you to attach an antenna in order to increase signal range. The Orinoco RG-1000 is priced at $230 but can be found online for around $160. (There are websites that discuss upgrading the firmware of your RG-1000 access point, you can do so at your own risk, check out http://www.icir.org/fenner/airport for more info.)

You don't need an Apple computer to configure the Airport Base Station. You can use Freebase, a free utility that allows you to configure your base station from a PC. (http://freebase.sourceforge.net).

Another good Access point is the Linksys WAP11. Its retail price is $220, but you can find it online for around $120. The WAP11 is a sound choice and features removable antennas. **NOTE :** the WAP11 is just a "Wireless to Ethernet" bridge. It is not a NAT router, or DHCP server. If you don't have a router, or DHCP server, you will need more than just the WAP11. The WAP11 can be used in conjunction with other "Home Routers" from Linksys, Dlink, SMC, etc.

On the higher end there is the Cisco Aironet 350 Series. This Access Point offers higher transmit power, 100-mW, compared to 30-mW of transmit power found on the Orinoco Access points, and even less for Prism Based Access Points (Linksys, Dlink, SMC, etc.)

These are just examples of quality access points. You can see reviews for many other Access Points on the "Practically Networked" website (http://www.practicallynetworked.com) and on the "Small Net Builder" website (http://www.smallnetbuilder.com).

3.2 With Firewall Capabilities.
There are many different types of firewalls; different access points use different types as part of their firewall protection. The next version of this document will contain a list of Access Points with built-in firewall protection and their respective functions.

It is noteworthy, however, that whenever you make your network available for public usage, without setting up any firewall protection you are as vulnerable as if the remote user were plugged in to your local LAN.

3.3 With Print Sharing.
D-Link DI713P supports print sharing, for example. Practically Networked lists many others.

3.4 With Standalone Repeating.
Standalone repeating allows you to set up an Access Point to "repeat" the wireless signal it receives from an existing Access Point. This is very useful if you want to extend the range of your wireless network by strategically placing these "standalone repeaters." Standalone repeating tends to be found in higher-end Access Points, such as the Cisco 350.

4. **Antennas & Amplifiers.**
To add range to your Access Point you need to connect an External Antenna. This will at times significantly increase your signal strength, and will allow for greater coverage area for your public node. With Standard Access Points, it is one antenna per Access Point. Some higher-end Access Points have dual radios built-in, so you can cover two areas with two antennas. An example of such is the Orinoco AP-1000.

Please note that there are many factors involved in increasing range, and what may work for one user may not work for another. The only way to truthfully determine what would work best for your node would be to have a site survey done. You can request for a site survey to be done in the NYC metro area by sending an e-mail to the NYCwireless mailing list. (http://lists.nycwireless.net/mailman/listinfo/nycwireless).

4.1 External connectors, pigtails, etc.
Access Point > Pigtail > low-loss Cable > Antenna. (Orinoco, Airport Base Station)
For the Orinoco and Apple Base stations, you need to purchase a "pigtail." This pigtail serves as an external connector. This allows you to connect an antenna. These pigtails are available online, for around $25 plus shipping (http://www.antennasystems.com/broadband.html#anchor37473).

Orinoco "Pigtail" external antenna connector

nycwireless

4.1 External connectors, pigtails, etc. (Continued from page 4)

Some Access Points have the connector built-in, such as the Linksys WAP11. In that case you don't need a "pigtail." You simply screw off the antenna that ships with the system, screw in the connector from the cable, and on the other end of the cable, connect it to an antenna and you are set.

If you want to place your Access Point further than the pigtail length (up to 3 feet), you would need a low-loss cable. This is because the type of cable used in the pigtail is considered a high loss type of cable so one would not want to have 25 feet of it, since you would lose all the antenna signal gain on the cable length. So, we utilize lower loss cable for greater cable lengths, such as LMR-400. You can purchase these cables, complete with connectors attached online (http://www.techsplanet.com/cables.htm) or if you are handy, and you have the tools you can make them yourself at a much lower cost. The Orinoco pigtails use the N-type connectors, the Linksys WAP11 external connectors use RP-TNC connectors.

How-To attach a "Pigtail" to an Orinoco RG-1000.

To attach the pigtail for the Orinoco and Apple Airport Base Stations you need to access some of the internal components. This might void your warranty. Use caution when opening up these devices.

For the RG-1000 and many other Access Points that use the same form-factor, first disconnect the AC adapter and remove the rubber cushion at the bottom. Use a small screwdriver to push in the little tabs. Once all three tabs are depressed, carefully removed one side of the case. Slowly work it side to side, and then it will pop off and you'll see the standard PC Card in the RG-1000. On the RG-1000, it is an Orinoco Silver PC Card. On the RG-1100, it is an Orinoco Gold PC Card. Then pop the pigtail connector off the end, and you can now connect the pigtail. If you do not use the modem, you can move the modem jack to the inside of the case, and tape it down using electrical tape and then you shall have an opening for the pigtail to exit the case without cutting a hole in it.

4.2 Directional and Omni-Directional Antennas.

A great source for directional antennas would be SuperPass (http://www.superpass.com). They have a large variety of different antennae for the 2.4 GHz spectrum. The next version of this doc will deal with proper antenna choice, based on where you place your Access Point and the area you intend to cover.

4.3 Yagi Antennas.

Can be obtained at Superpass.com or dBiplus.com. You can also make one out of a Pringles can. The whole process takes a few hours after you buy the necessary parts. You can also post to the NYCwireless list and inquire to find out if anyone has any extra parts for it. (http://www.oreillynet.com/cs/weblog/view/wlg/448).

4.4 Using Amplifiers.

Amplifiers can be used to significantly increase signal strength. There will be more discussion on this topic in the next version of the doc.

5. Network Setup and Security Basics.

You need to have the proper network settings in order to share your Internet connection, as well as to distribute IP addresses automatically using DHCP. We will also touch on a few basics regarding security.

5.1 Typical Network Configurations.

Many ISPs will give you a single public IP Address. To set up multiple computers to access the Internet, while appearing to originate from that single IP address, routers use Network Address Translation (NAT). This allows you to assign your own internal addressing while allowing you to access external resources such as the Internet.

Common internal network addresses are 192.168.x.x, 10.x.x.x., and 172.16.x.x.

5.2 Basic Security Issues.

If you are sharing your home network with the public, i.e. you are on the same network segment, use common sense security as you would with any unknown user who plugs into your LAN.

Even if you are not on the same segment, as long as your data is not encrypted, someone can “sniff” that data if your wireless network is “open.” (Being closed, i.e. using WEP, is not exactly secure, as there are known methods to crack the WEP “security”).

[Adapted from the NYCwireless FAQ]
Users are advised to use SSL to connect to web pages and mail hosts, SSH instead of telnet whenever possible, and VPNs (virtual private networks) for all other data to ensure privacy and security.

6. Typical Access Point and Client Card Configuration.

You need to set up your Access Point properly so that others can easily connect to your network.

6.1 Common Access Point Configurations.

Have the following info properly input in Your Access Point:
Router Address or Gateway: This is the IP Address assigned to you by your ISP.
DNS: These addresses are provided by your ISP.
Enable DHCP and NAT.
Set your SSID to www.nycwireless.net .
Make note of the channel on which you are broadcasting. Not all clients can channel hop to the appropriate channel.

6.2 Common Client Card Configurations.

Make sure to have your TCP/IP settings set to obtain an IP Address automatically (DHCP). Have your ESSID (or SSID, Network Name) set to “any” or to www.nycwireless.net so you can automatically connect to the networks.

6.3 How-To connect to an NYCwireless Network (Mac OS 9.x)

Connect to the NYCwireless network using Mac OS 9.x

.:. At the "Apple Menu" select "Airport."
Expand "Settings." It should read "AirPort: On." If it is "Off" click on "Turn AirPort On."

.:. Under "Choose network" select "Other."
For the "network name" type in - www.nycwireless.net - leave the password field blank, and click on "OK."

.:. At the Apple Menu select "Control Panels" and select "TCP/IP."

.:. Select "Connect Via" and choose "AirPort" from the drop down menu.
In the "Configure" menu, select "Using DHCP Server."

.:. Close the window and when prompted, save the changes.

Launch Your Web Browser.

6.4 How-To connect to an NYCwireless Network (Mac OS 10.x)

Connect to the NYCwireless network using Mac OS X

.:. At the "Apple menu", select "System Preferences" (appears in the upper left of the screen display).
Select "Network."

.:. Verify that "Show": is set to "AirPort".

.:. Select the "TCP/IP" tab.
The settings should appear as follows:
Configure: Using DHCP
The Domain Name Servers (Optional) should be left blank.
The DHCP Client ID: should be left blank.
The Search Domains (Optional) should be left blank.

.:. Select the "Airport" tab.

Preferred Network should be set to - www.nycwireless.net -. The Network password should be left blank.

.:. Click "Save."

Under "System Preferences", select "Quit System Preferences."

Launch Your Web Browser.

7. Node Auditing / Site Surveying.

The purpose of the node audit is to ensure that your node is operational and available for public use. It is also helpful to insure that your wireless coverage is providing maximum coverage. Node Auditors are individuals that travel around an area to test the nodes that are listed in the maps database so to determine that they are both operational and have sufficient signal coverage for public use. Please contact Ben Serebin (ben@nycwireless.net) if you would like to volunteer as a Node Auditor.

7.1 NetStumbler Usage.

After you initially setup your Access Point (and possibly antenna), the next step is to check the coverage of the area to which you are attempting to provide wireless access. Use NetStumbler to check signal coverage and open networks around you. You can download NetStumbler from the NetStumbler website (http://www.netstumbler.com). There are versions available for Microsoft Windows 9x/NT/2000/XP and for Microsoft Pocket PC.

7.2 Improving your antenna / AP positioning.

Walk around the area you are attempting to cover, and verify that you have good signal strength. Ideally your location overlooks the area you are attempting to cover with wireless coverage. The ideal location for an antenna or AP is a window (you won't have to worry about water damage or other weather related issues). This window should not have metal shielding, Venetian blinds, screens, or other types of obstructions. All of these will reduce the signal strength. Be aware of foliage during the spring and summer seasons. They tend to decrease signal strength.

7.3 List or update the node in the maps database.

After you have verified your signal coverage of a location, list your node in the maps database. This is a crucial step to maximum usage of your node and to expand the network. Also, be sure to state the coverage and the date of your audit.

8. Credits and Glossary of Terms.

Getting Started with Free Wireless Networks version 0.7.8
Author, Editor: Jacob Farkas.
Glossary by Ben Serebin.
Jacob Farkas, Ben Serebin and Terry Schmidt contributed to the content of this document. There is an online version available for viewing, editing, etc. (http://www.freenetworks.org/moin/index.cgi/CookBook). For any questions or comments please e-mail jacob@nycwireless.net.

Glossary of Terms

Access Point (AP) - A wireless LAN transceiver that acts as a center point of an all-wireless network or as a connection point between wireless and wired networks.

Antenna - A device for transmitting or receiving a radio frequency (RF). Antennas are designed for specific and relatively tightly defined frequencies and are quite varied in design. An antenna designed for 2.4-GHz 802.11b devices will not work with 2.5-GHz devices.

Bandwidth - Specifies the amount of the frequency spectrum that is usable for data transfer. It identifies the maximum data rate that a signal can attain on the medium without encountering significant loss of power.

Client - Any computer connected to a network that requests services (internet access, files, etc.) from another member of the network.

Glossary of Terms (continued from page 7)

Client Adapter - Network interface card that provides devices with wireless connectivity.

Directional Antenna - An antenna that concentrates transmission power into a direction such that coverage distance increases at the expense of coverage angle. Directional antenna types include yagi, patch, and parabolic dish.

Dynamic Host Configuration Protocol (DHCP) - A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on a network. The device retains the assigned address for a specific administrator-defined period.

Gateway - A network point that acts as an entrance to another network.

Network Address Translation (NAT) - The translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the internal network and it appears as one entity to the outside world. In the case of wireless LANs with an outside Internet connection, the NAT capability of Internet-sharing software allows the sharing of one Internet connection among all the wireless PCs connected.

Patch Antenna - A type of flat antenna designed for flush wall mounting that radiates a hemispherical coverage area.

Roaming - Movement of a wireless node between two access points. Roaming usually occurs in infrastructure networks built around multiple access points.

UPS - An uninterruptible power supply (UPS) is a device that allows your computer to keep running for at least a short time when the primary power source is lost. It also provides protection from power surges. A UPS contains a battery that "kicks in" when the device senses a loss of power from the primary source. When power surges occur, a UPS intercepts the surge so that it doesn't damage your computer.

Wireless Node - A user computer with a wireless network interface card (adapter).