User Manual - AirStation WHR-HP-G54

High-Power Wireless SmartRouter

Table of Contents

Work and play - further and faster! Eliminate dead spots and enjoy faster connections with extended range with your new *AirStation High Power Wireless SmartRouter.*

System Requirements

- A high-speed (Broadband) Internet connection or existing local area connection.
- A computer with an Ethernet port and a web browser such as Firefox, Internet Explorer, Opera, or Safari.

Package Contents

- WHR-HP-G54 AirStation
- Antenna
- Optional Base
- AC adapter and power cable
- CAT5 LAN cable
- Utility CD with Manual
- Quick Setup Guides
- Warranty Statement

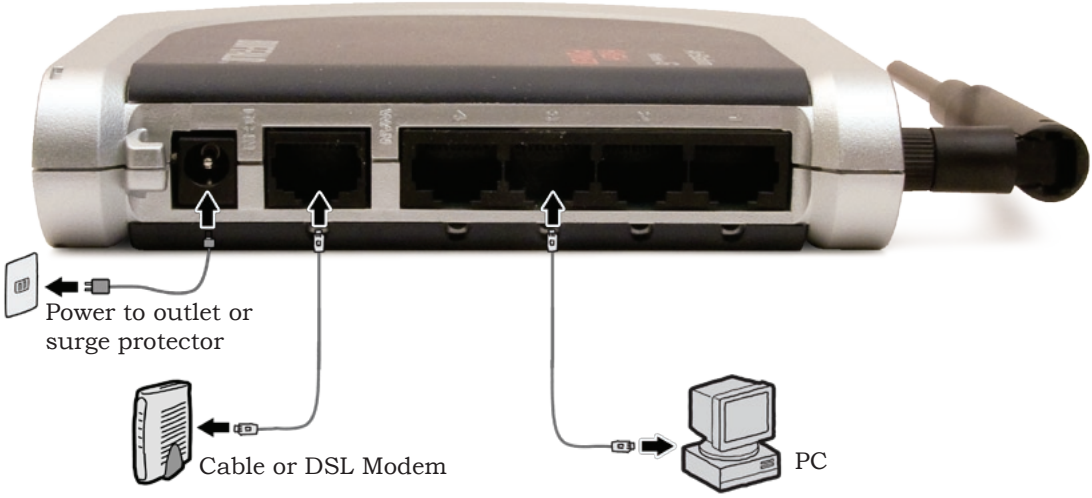
Begin by finding a good place to set up your router/access point. Some things to consider:

- You'll need to be able to plug your internet connection into it, so it should go within reach of the LAN cable from your DSL or Cable modem. You'll also want a power outlet nearby.
- Keep the access point as central in your work area as possible. Signal strength and speed fall off with distance.
- Higher is often better. For instance, set it up on the top shelf of a bookcase rather than the bottom one, if possible.

Do you need a password or other information to log in to your internet connection? Many DSL connections require information like global IP address, subnet mask, default gateway address, DNS server address, or PPPoE parameters in order to connect. Cable modems usually don't require extra information. If you have a DSL internet connection, make sure that you have any necessary information handy before you continue. Your Internet Service Provider can give you this information if you don't know it.

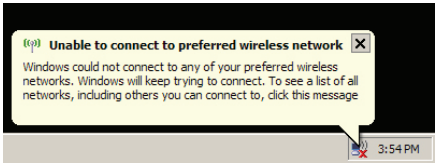
The AirNavigator CD can install your AirStation for you automatically. To use the automatic installation program, insert your AirNavigator CD into your computer and follow the onscreen directions.

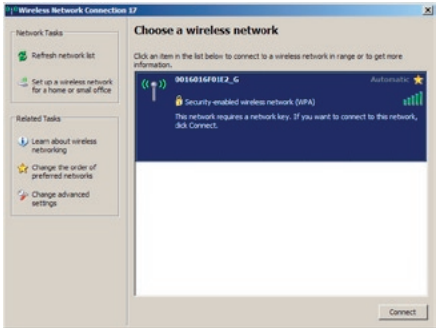
The wizard will guide you through installing your AirStation. You will have the opportunity to change your admin password, personalize your SSID, and set up WEP128 encryption.


Power to outlet or
surge protector
Cable or DSL Modem
PC

To install the AirStation manually,

1. Power down the Cable or DSL modem and the computer which will be used to configure the AirStation router.
2. Plug the Cable or DSL modem's Ethernet cable into the AirStation's WAN port. Initially, you may need to unplug this cable from your computer, hub or other router.
3. Plug the provided Ethernet cable into one of the four LAN ports on the AirStation and plug the other end into your computer's Ethernet adapter (NIC).
4. *Important: turn everything on in the correct order!!* Power on your cable or DSL modem and wait one full minute, then power on the AirStation and wait one full minute, and finally power on the computer which will be used to configure the AirStation.





To connect wireless devices to the AirStation, you may either enter the SSID and encryption key manually, or you can use AOSS to automatically configure your wireless settings.

If you used Automatic Installation with default settings, then your AirStation's SSID is "Buffalo", and the encryption is 128-bit WEP with the 13 digit key that you specified.

Consult your wireless clients' manuals for instructions on configuring them manually.

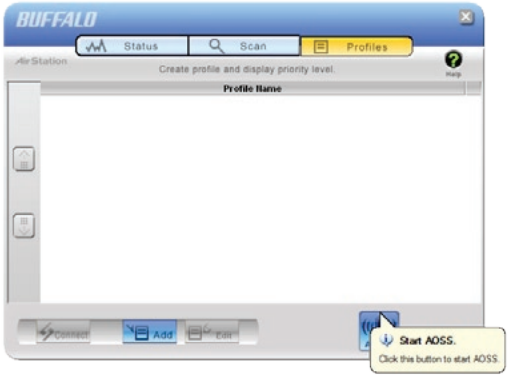
To use AOSS to configure your wireless clients automatically, turn to the next page.

AOSS (AirStation One-Touch Secure System) is a simple system for configuring your wireless network securely. If your router and your client device are installed and both support AOSS, then making a secure wireless connection between them is very easy.

Push the AOSS button on the top of your router and hold it in for a few seconds. The AOSS light will begin to flash. You now have two minutes to push the AOSS button on your client device and finish the connection.

Some client devices have a red button labeled "AOSS". If yours is one of these, push the button! About 15 seconds later, you'll have a secure network connection.

For client devices without a physical button, use the AOSS button in the Client Manager software. Check your client device's user manual for instructions on where to push or click the AOSS button.



After you've pressed both buttons, it will take about 15 seconds for the connection to complete. When it's finished, the AOSS light will glow a solid amber. You now have a secure network connection!

Some things to keep in mind when automatically connecting with AOSS:

- Only one wireless client adapter can be configured with AOSS at a time.
- It is not necessary to reconnect client devices that have already been configured via AOSS unless significant changes have been made to the wireless network.
- Do not attempt to configure two separate AOSS networks at the same time, as it may cause undesired configurations.
- If an undesired client has connected via AOSS, it can be disconnected from within the WHR-HP-G54's web-based admin tool.
- Even if your client device doesn't officially support AOSS, you may still be able to use AOSS if you install Buffalo's Client Manager software on your computer. It works with most client devices, including many made by other manufacturers. You can download it from *www.buffalotech.com*.

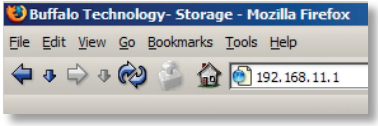
This AirStation supports quickly changing the product from a wireless router to a conventional access point.

Put your Airstation into Access Point Mode by moving the switch on the bottom of your AirStation from AUTO to BRI. This changes the default IP address of the AirStation from 192.168.11.1 to 192.168.11.100, and DHCP, NAT, and the WAN port are disabled.

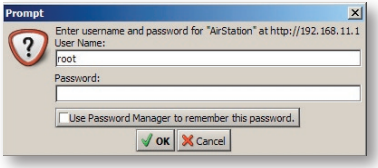
Access Point Mode might be desirable if you're adding wireless capability to an existing network with a router, or configuring your AirStation as part of a repeater bridge setup. It is not suitable for most home configurations. If you plan to use the AirStation as an normal wireless router, make sure that this switch is in the normal (AUTO) position!

Instructions for configuring multiple AirStations in a wireless bridge can be found in the 'WDS Bridging' section of this guide.

The Web Admin Tool allows you to easily change the settings for your AirStation. To use it, launch a web browser on a computer connected to the AirStation.



Enter the AirStation's LAN-side IP address into the URL field. By default, this will be *192.168.11.1*.

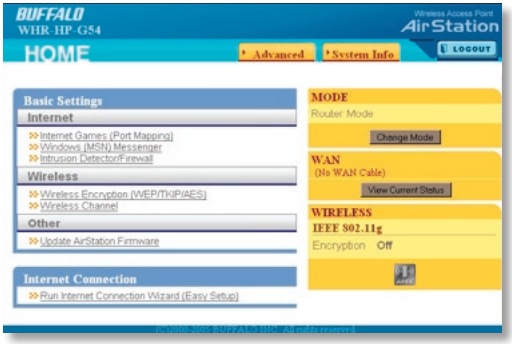


A window will open, prompting you to enter a User Name and Password.

The User Name is *root*. By default, the password is blank.†

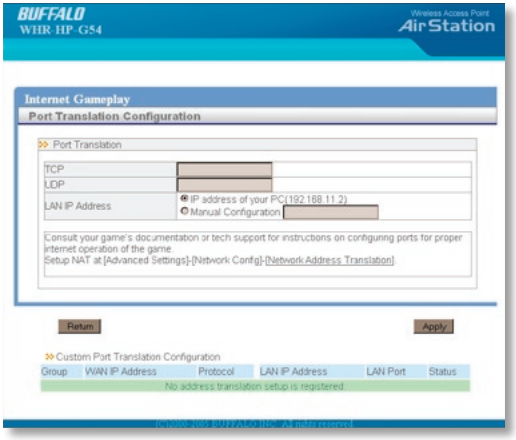
*In AP mode (mode switch *BRI*), the default IP address is 192.168.11.100.

†If you ran the Automatic Installation program, you may have changed your password for the Web Admin Tool. If so, use the password you set. To reset the password to a blank field, hold down the Init button on the AirStation until the Diag LED flashes.

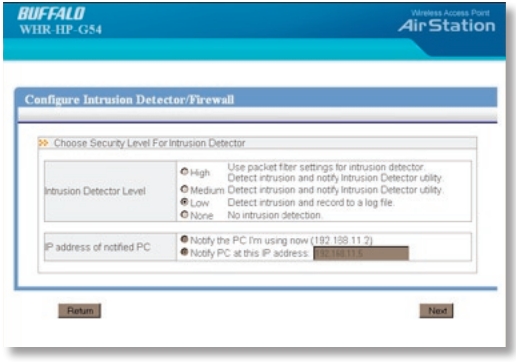


When you first open your AirStation Configuration Tool, it takes you to its *Home* page. From Home, you can configure *port mapping* for your internet games, set UPnP for *Windows (MSN) Messenger*, configure your *firewall*, setup *encryption*, choose your *wireless channel*, update your AirStation's firmware, and reset your *Internet Connection*'s configuration. Clicking the *Advanced* tab gives you access to all of the AirStation's configuration tools.

You can get back to Home from anywhere in the management tool by clicking on the *Home* button at the top left of the screen.

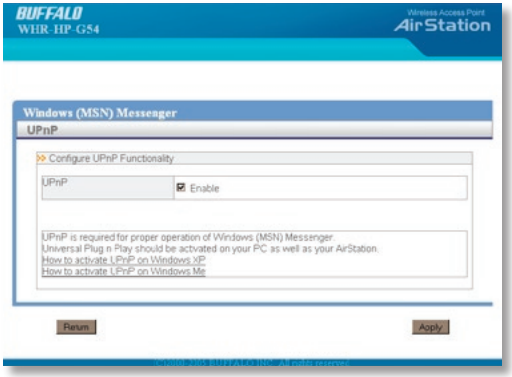


Select any ports that need to be opened for your internet games to function correctly. Consult your game's documentation for more information on what ports need to be configured.



From this page, choose the level of firewall security you desire. You may also choose to have alerts sent to a different PC, if you like. Click *Next* when done to restart the router.

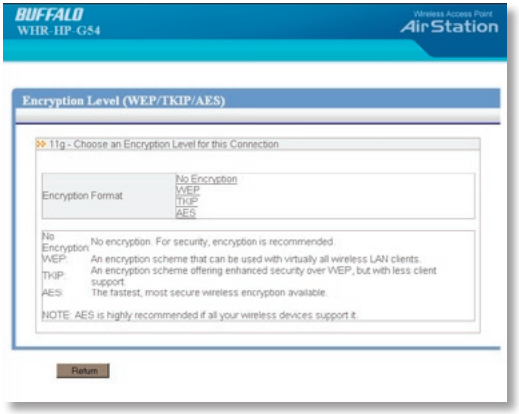
Get to this page from Home by clicking on *Firewall/Intrusion Detector.*



Windows (MSN) Messenger requires UPnP for proper operation. You may *Enable* UPnP here. UPnP may need to be configured on your PC as well.

If you need to configure UPnP on your PC, the links at the bottom of the page have instructions for doing so on Windows ME and XP computers.

Get to this page from Home by clicking on *Windows (MSN) Messenger*.

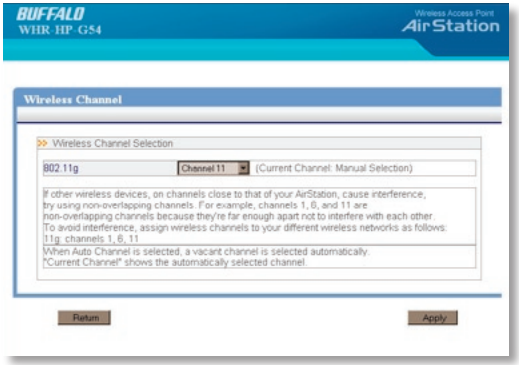


This page is available from *Home* by selecting *Wireless Encryption*. Here, you can manually select the type of wireless encryption you'd like to use. Your AirStation supports three different encryption schemes; choose the best one that all your clients support.

Virtually all wireless clients support ***WEP***. It's better than nothing.

TKIP is more secure than WEP, but some wireless clients don't support it.

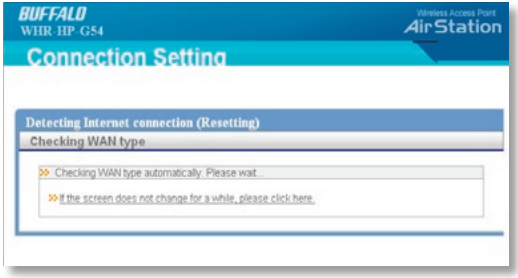
AES is even more secure. It should be your first choice if all of your clients support it.



This page is available from *Home* by selecting *Wireless channel*. With *Auto Channel* selected, your AirStation will choose the best channel available. *Current channel* will show the channel that your AirStation is currently using.

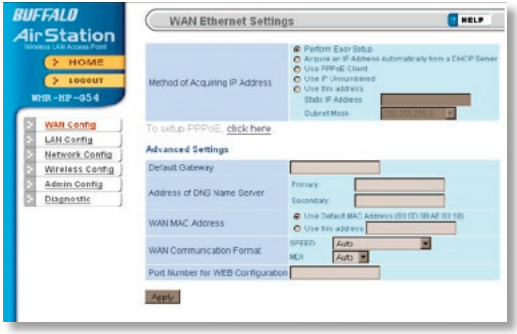
You may also select any channel from 1-11 manually. Channels 1, 6, and 11 are non-overlapping. If multiple channels are in use in an area, select a different channel for your AirStation, as far away from the other channels being used as possible.

This page is available from *Home* by selecting *Firmware update*. Use *Browse* to select your firmware update file, and then click on *Apply*. Firmware update may take several minutes to complete. Don't power down your AirStation until the diag LED has gone out.



From *Home*, selecting the *Internet Connection Wizard (Multisession Reset)* tab will begin the Internet Connection Wizard.

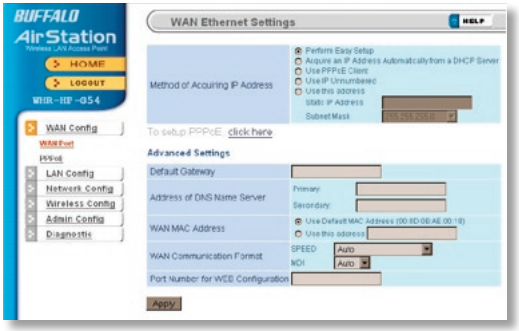
The Internet Connection Wizard will only function correctly in simple networks, where your cable or DSL modem is plugged directly into your AirStation's WAN port. If you have a complicated existing network that you're adding the AirStation to, see page 55.



Advanced Settings lets you configure every element of your AirStation. Get to Advanced Settings from Home by clicking the *Advanced* Tab. You may return to Home by clicking on the yellow > *Home* link in the top left corner.

Click *Help* in the top right corner for more information about any of the pages in Advanced Settings.

To begin, click on *WAN Config*. The first page in WAN Config, *WAN Port*, will open.

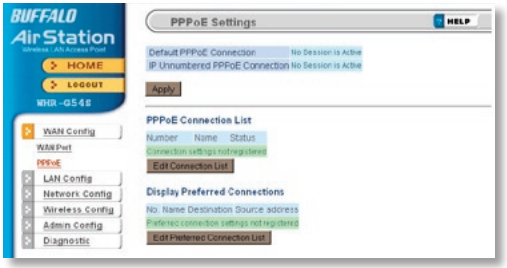


Here, you may choose how the AirStation acquires an IP address. Normally, the internet connection wizard will set this for you if you have a cablemodem or DSL. If you're not sure what to choose, perform *Easy Setup*.

To setup PPPoE manually, click on *click here* and turn to the next page.

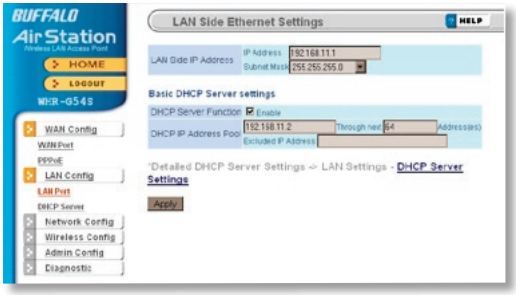
Also on this page, under *Advanced Setup*, you may manually set the Default Gateway, DNS server, WAN MAC address, WAN format, and WEB port number.

Click *Apply* when finished.



Many DSL connections require a PPPoE Connection in order to log in to an internet connection. Normally, the Easy Detection Wizard will help you configure that, but you may manually configure one here. Consult your ISP for more information on correctly configuring your PPPoE connection.

To add a new PPPoE connection, click *Edit Connection List*. To choose your preferred connection, click on *Edit Preferred Connection List*.



Default for the *LAN side IP address* is 192.168.11.1. To add the AirStation to an existing LAN, specify a unique IPaddress, not used elsewhere in the network.

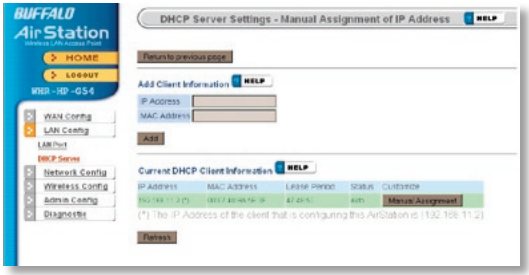
The default Subnet Mask is 255.255.255.0. To connect AirStation to an existing LAN, specify the Subnet Mask that the LAN uses.

If there's more than one DHCP server on a network, disable all but one of them. To have DHCP assign addresses from a specific range, enter a beginning address by *Assigned IP Address* and give the number of addresses to assign in the *Addresses* box. To exclude specific addresses from being assigned by DHCP, specify them in the *Excluded IP Address* box. Multiple IP addresses may be specified by separating them with a comma, e.g. 192.168.11.7,192.168.11.9. You can also specify an IP address range by start and end address connected by a dash, e.g. 192.168.11.15-192.168.11.21. The ',' and '-' can be used at the same time, e.g. 192.168.11.7,192.168.11.9,192.168.11.15-192.168.11.21, up to a total string length of 128 characters.

Click the *Help* link in the top right corner for more information.

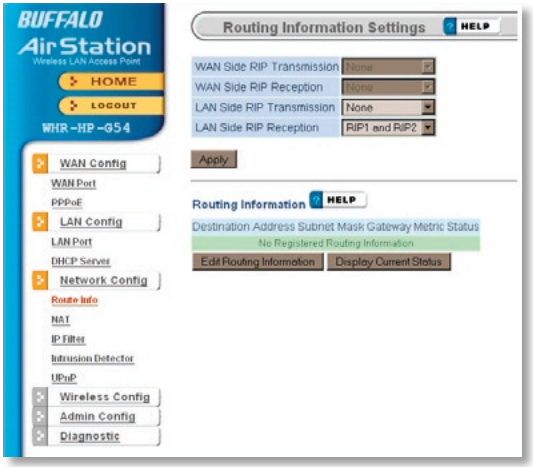
This page offers the same DHCP settings as the previous one, and in addition, offers you the chance to change the *Lease Period*, *Default Gateway*, *DNS servers*, *WINS server*, and *Domain Name*. Click *Apply* when you have the settings the way you want them.

To manually assign an IP address, click *Manual Assignment*.



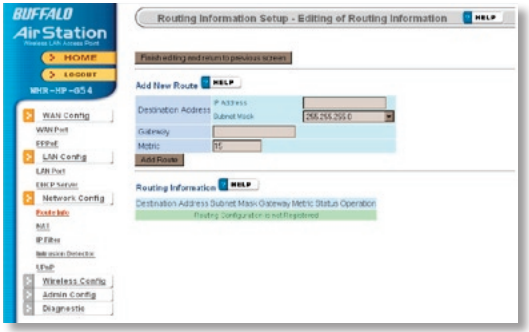
To manually link a LAN address to a MAC address, enter them under *Add Client Information* and click *Add*.

Current DHCP Client Information shows all LAN addresses currently assigned by AirStation's DHCP. You may configure a specific client to always receive the same IP address by clicking *Manual Assignment* to the right of its MAC Address. Clicking *Delete* returns a manually assigned client to normal DHCP operation. *Edit* allows you to manually adjust a linked IP Address and Mac Address in the Client Information window above.

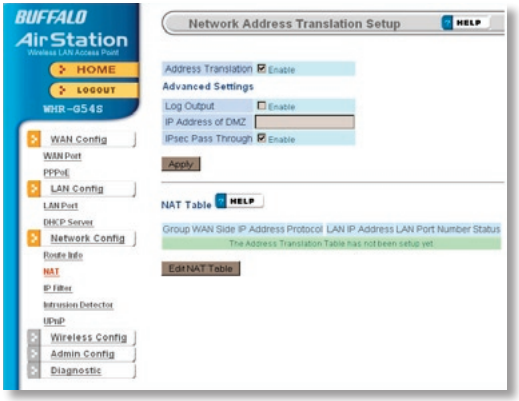


By default, the AirStation receives RIP (Route Information Protocol) information only from your local network, and doesn't broadcast RIP at all. For large, complicated network configurations, you may wish to modify this behavior. Click *Apply* when you have your desired configuration.

Lower on the page, routing information is displayed. Click *Edit Routing Information* to add a new route manually.



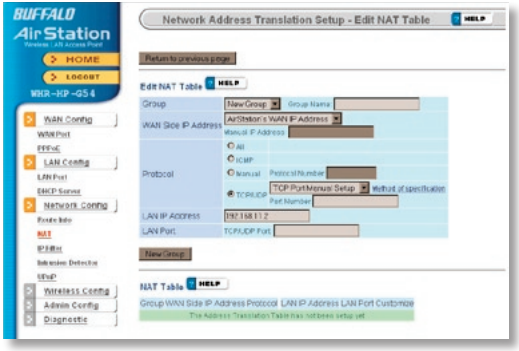
To configure a route manually, enter its *Destination Address* and *Gateway*. Enter a maximum number of hops allowable in *Metric* and click *Add*.



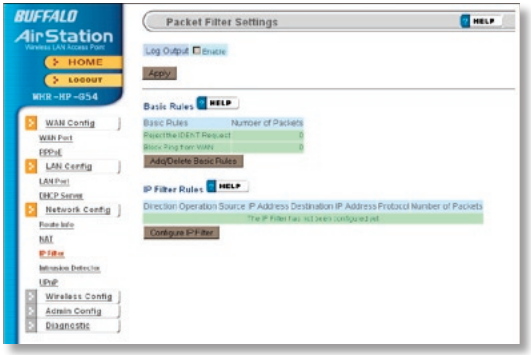
You may disable Network Address Translation and IPsec passthrough by unchecking the appropriate *Enable* boxes. If you have a DMZ, enter its IP address in the *IP Address of DMZ* box. Incoming packets containing no recognizable destination port information will be redirected to the DMZ's IP address.

Click *Apply* when done.

To set a NAT table entry manually, click *Edit NAT Table*.

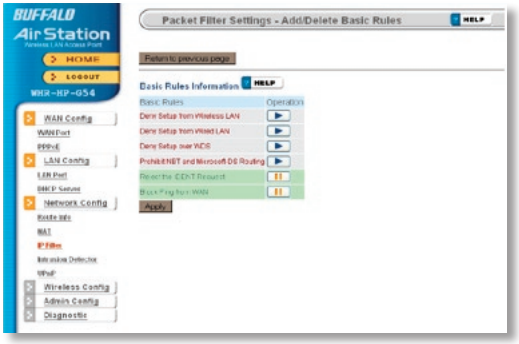


From this page you may manually add entries into the Address Translation Table. Click *Add New Group* when each is complete.

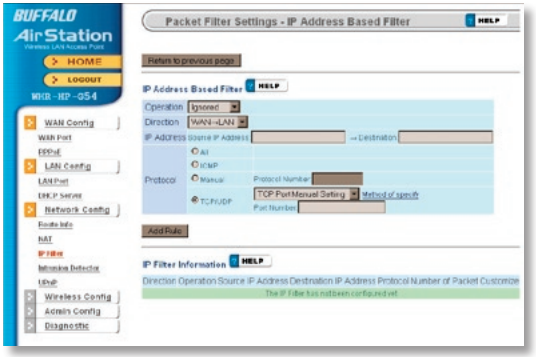


Your AirStation comes pre-configured with basic rules. You may choose which of these to use by clicking on *Add/Delete Basic Rules* and turning to the next page.

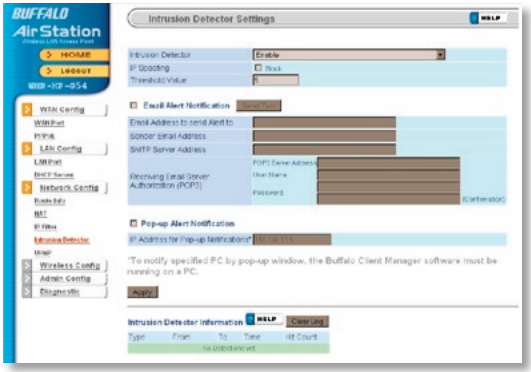
To make a custom rule, click on *Configure IP Filter* (page 35).



Get here by clicking on *Add/Delete Basic Rules* from the previous page. You may choose which of AirStation's preconfigured basic rules are enabled or disabled. Active rules are displayed with a green background, and disabled rules are shown in red. Choose the rules you want to use by clicking under *Operation*. When your choices are complete, click on *Initialize*.



Clicking on *Configure IP Filter* from the IP filter page (page 33) will bring you to this page, where you can make your own rules. Click *Add Rule* when you have each rule configured the way you want it.



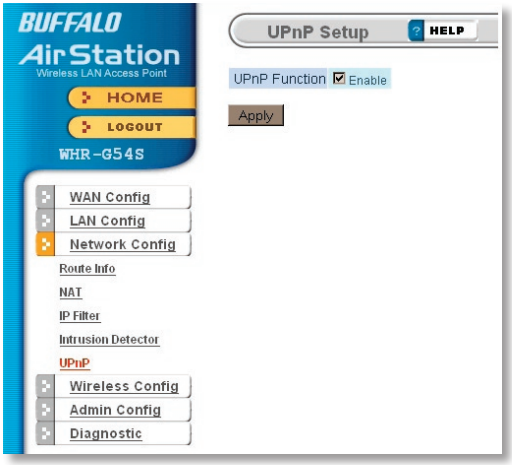
To enable intrusion detector, choose *Enable* or *Enable (Apply packet filter rules)* from the Intrusion Detector drop-down box. If packet filter rules are applied, packets will be filtered with packet filter rules before Intrusion Detector is applied.

Blocking IP spoofing blocks packets from devices using an IP address that is not their own.

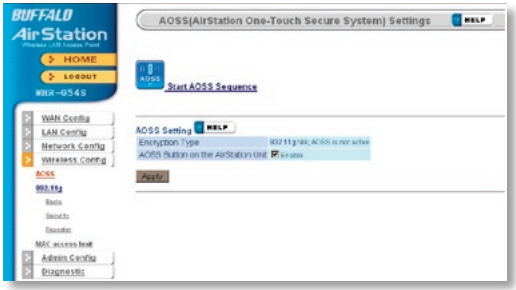
In the *Threshold Value* box, enter the number of times an event has to occur before you receive notification.

To configure your email alerts, enter your email address and mail server information. You may make up a sender email address, such as “alert@router.com”. Alert emails will appear to come from this address.

Intrusion detector also blocks unauthorized access attempts and suspicious traffic from WAN-side devices (the internet).



You may disable Universal Plug and Play functionality by unchecking *Enable* here. Note that Windows Live™ Messenger may not function correctly with UPnP disabled.

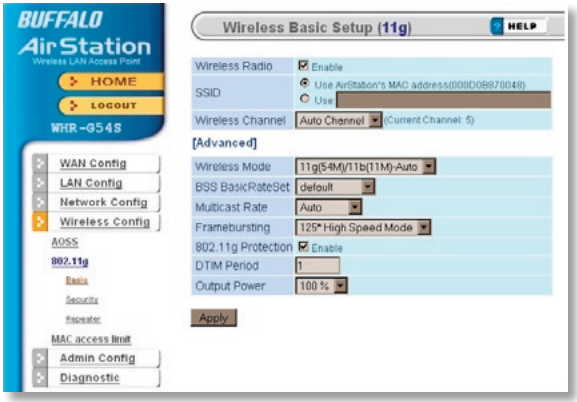


Clicking *Start AOSS Sequence* has the same function as pushing the AOSS button on the router: it initiates the AOSS process.

If all your clients support AOSS, it's very simple to set them up. Press the AOSS button on the router, or the one on this page, and then push the AOSS button on the client device.

Each client device will have to be set up separately. Wait for each AOSS process to finish before starting the next one.

Consult your client device's documentation for the location of its AOSS button.

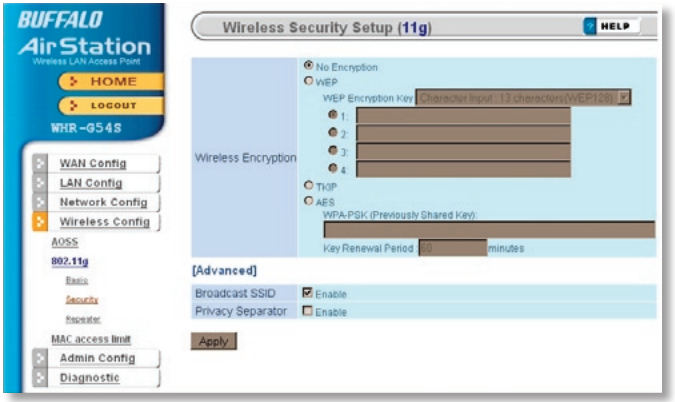


If you have a mixed mode network, with both 802.11b and 802.11g clients, it's recommended that you check *11g protection* to ensure that slower 11b clients don't hog all available bandwidth.

Choosing *Auto* for *Wireless mode* lets both 802.11b and 802.11g clients connect to the network. If you would prefer to allow only one or the other, you have those options as well.

Two different framebursting modes are available. These can double throughput in your network if all clients are configured to use them. *125* High Speed Mode* is an improved version of *Frameburstring* and is highly recommended if your clients support it. If a framebursting mode is enabled and some of your clients don't support it, it simply won't be used.

Reducing the *Output Power* below 100% will reduce the range of your router. Setting it to 0% shuts down the AP part of the AirStation completely.



Buffalo recommends that you choose the strongest form of encryption that's supported by all your client devices.

- *WEP* is better than nothing, and almost every wireless device ever made supports it.
- *TKIP* is slower than WEP but much more secure.
- *AES* is the most secure of all. It should be your first choice if all of your devices support it.

Setting the key renewal period too short can decrease network performance.

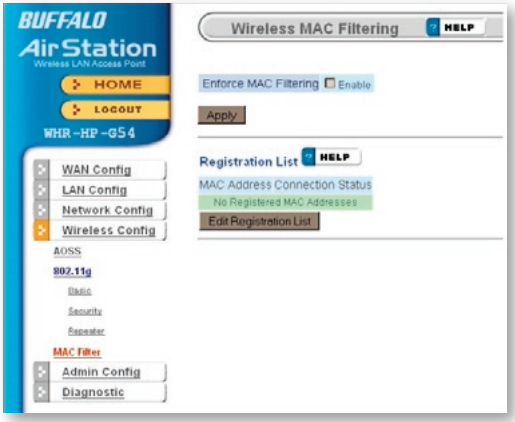
By default, the AirStation broadcasts its SSID. This makes it easier for clients to connect to the AirStation. To disable broadcasting, uncheck this box.

Privacy Separator prevents wireless clients from being able to browse each other's computers. Check *Enable* to turn it on.

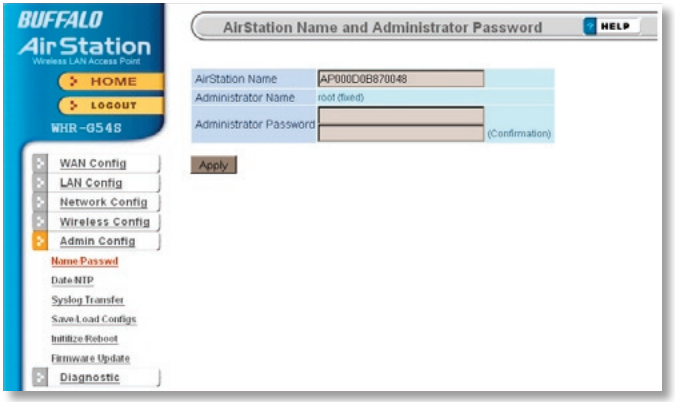
When configuring a bridge between two or more wireless access points, WDS must be enabled here.

For instructions on configuring a WDS bridge, see page 56, or click on *Help* at the top right corner of the screen.

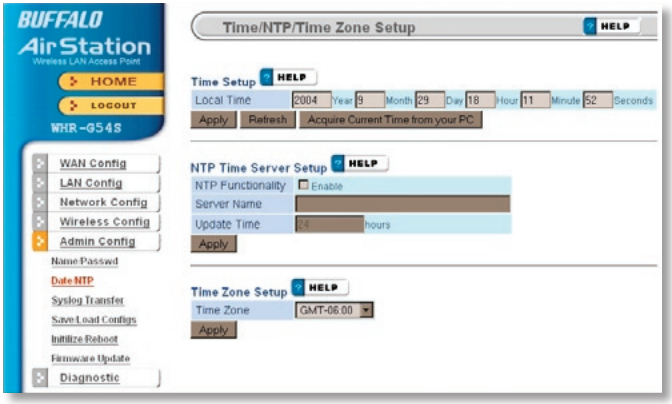
You may limit access to your wireless network to specific computers. Computers not listed on your MAC Registration List will not be able to connect to the network. If you enable this, click *Edit Registration List* to add MAC addresses to your registration list.



Enter a MAC address and click *Apply* for each client that's going to be accessing the network.



Here, you can change your AirStation's name on the network and the administrator password. The name of the administrator account is fixed as "root". If you have many AirStations on your network, having clear, descriptive names for each can make them much easier to administrate.

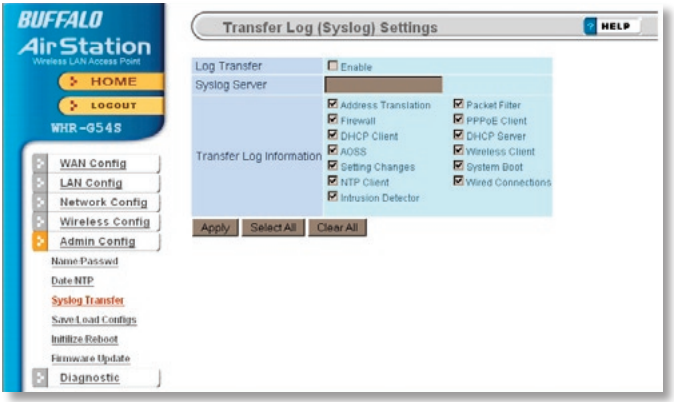


You may set the time and date on your AirStation by entering it manually, and then clicking *Apply*.

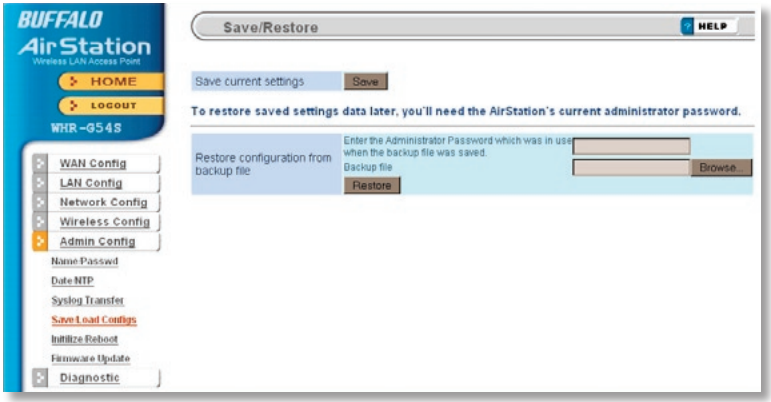
You may also click *Acquire Current Time from your PC* to set time and date automatically to match the PC you're using to set it up.

If you have an NTP time server on your network, *Enable* NTP functionality and enter your NTP *Server Name*. Choose how often you want time updated and click *Apply*.

If you're setting time manually, you'll need to select your Time Zone and click *Apply*.

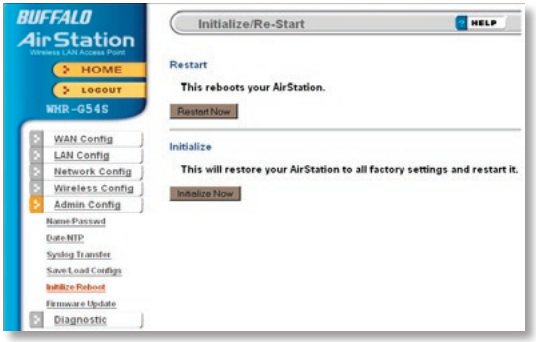


If you have a syslog server on your network, you may send logs to it. Check *Enable* to have logs transferred. Enter the address of your Syslog Server, check the logs you want transferred, and click *Apply*.



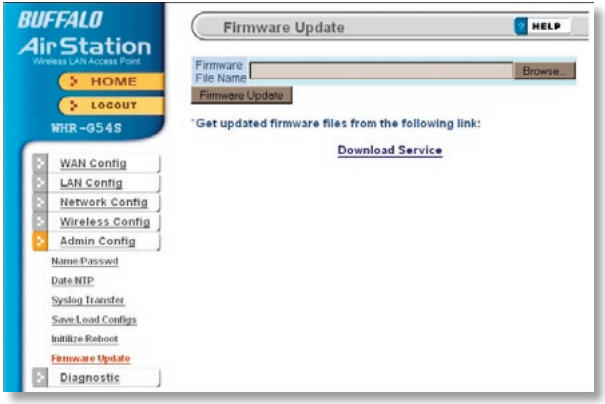
Once your AirStation's configured the way you want it, you can save the configuration here. You'll need the current administrator password to restore the configuration from the backup file later.

Click *Help* at the top right corner of the page for more information on backing up and recovering system configuration files.



Click *Restart Now* to restart your AirStation. Click *Initialize Now* to restore your AirStation to factory defaults and restart it.

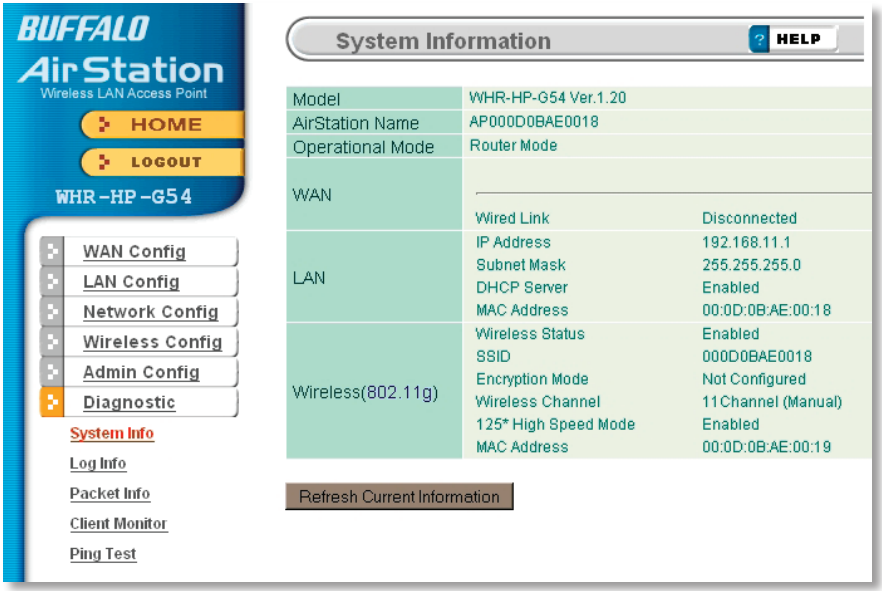
You may also initialize your AirStation by holding down the *Init* button on the bottom of the router for 3 seconds.



Click *Browse* to select your firmware update file. Then, click the *Firmware Update* button to update firmware.

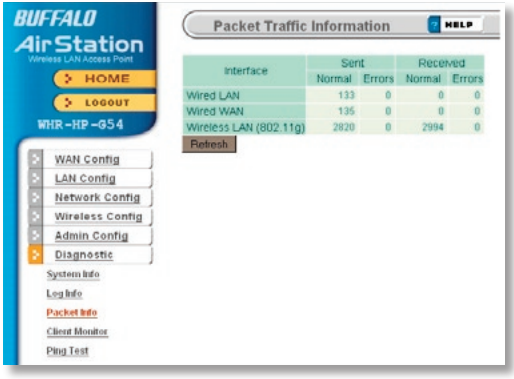
Firmware Update may take several minutes to complete. Do not power down the router until Firmware Update is finished and the diag light on the front of the router has stopped blinking.

When available, updated firmware may be downloaded from *www.buffalotech.com*.



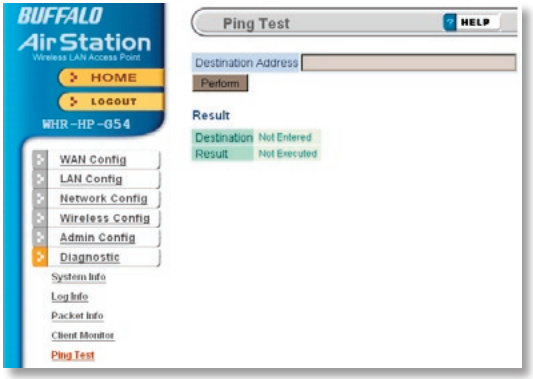
The System Information page lists all the setup information for your AirStation. It can be very handy for setting up clients that don't support AOSS.

Here you can choose what information gets logged and see recent log entries.



Here, you can see the packets and errors for each of your networks.

Client Monitor shows you a list of all clients currently connected to the wireless network.



To perform a *Ping*, enter a target (such as *192.168.11.2* or *www.buffalotech.com*) and click *Execute*.

Successful pings return "64 bytes from . . ." messages. If the ping returns "Connection failed" or other errors, something is preventing you from communicating successfully with your target.

To add an AirStation to a network without changing the existing LAN configuration, proceed as follows:

1. Put the AirStation in AP mode by moving the switch on the bottom from *AUTO* to *BRI*.
2. Connect one of the AirStation's LAN ports to an existing router or switch on your network.
3. Temporarily change your computer's IP address to an unused address on the 192.168.11.x subnet, with subnet mask 255.255.255.0.
4. Type "192.168.11.100" into a browser window to open the AirStation's Configuration Tool.
5. In *LAN Config*, configure the following settings:

   IP Address = [192.168.11.137] (Specify an unused network address from the existing LAN.)

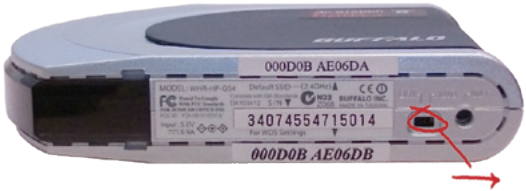
   Subnet Mask=[255.255.255.0] (Use the same Subnet Mask as the existing LAN.)
6. Restore your PC's IP address settings to their original values.

Your AirStation's WDS bridging capability allows you to extend the size of your wireless network by adding additional AirStations, all connected wirelessly.

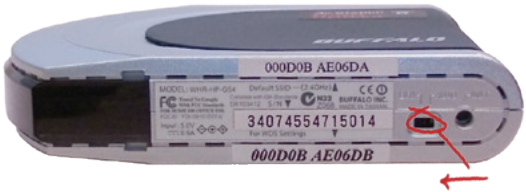
In this simple example, we'll connect two AirStations in a wireless bridge. You may use these same steps to add additional bridges for greater coverage.*

For easiest configuration, we recommend configuring all components in close proximity before deploying them to their final positions. Wired connections make initial configuration even simpler.

The first AirStation will be the router that receives the internet connection. On the bottom of the AirStation, make sure that the switch is set to "AUTO". If desired, you may connect the Ethernet cable from your cable or DSL modem to its WAN port now, though this is not necessary for configuration. Power on the first AirStation.



The second AirStation will be configured as a repeater/bridge. Make sure that its switch is set to "BRI". Use a RJ-45 cat5 Ethernet cable to connect LAN ports of the two AirStations. Power up the second AirStation.

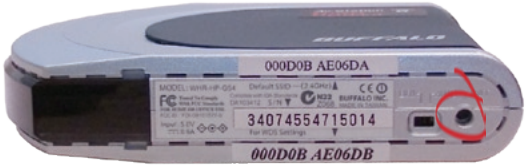


Connect a PC's Ethernet port to another RJ-45 port on the main router (the first AirStation). You will use this PC to configure the settings of the AirStations.

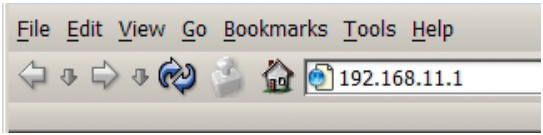
Here's the whole setup, ready for initial configuration.

* Note: Each AirStation may be part of 6 different bridges. Remember that each layer of bridges takes about half your total network speed, so avoid configuring daisy-chains more than 4 bridges long. A star-pattern is always better, with a central router serving multiple bridges.

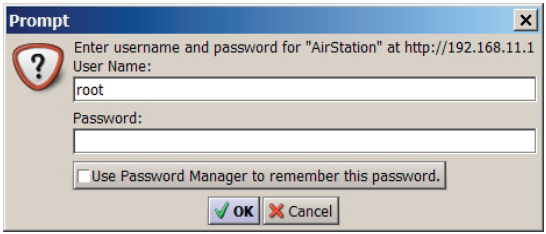
Once the AirStations are powered on, you will want to make sure that they are in factory default configuration. On the bottom of each, hold down the "INIT" button for three seconds. This will reset them to factory defaults. They will take 30-60 seconds to reboot afterwards.



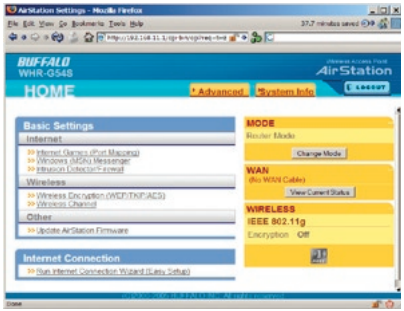
Power on your PC. Make sure that it is configured to "obtain an IP address automatically" from DHCP. Open a web browser and in the address field, enter *192.168.11.1*. This is the default IP address of your first AirStation.



A login window will pop up. The default username is "root". Leave the password field blank and click OK.

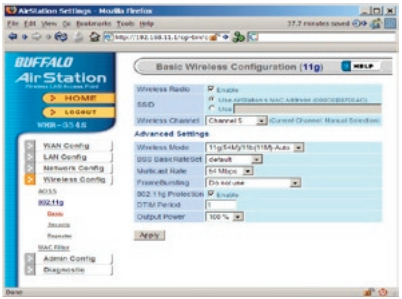


The Web Admin Tool for your first AirStation will open. Click on the *Advanced* tab.



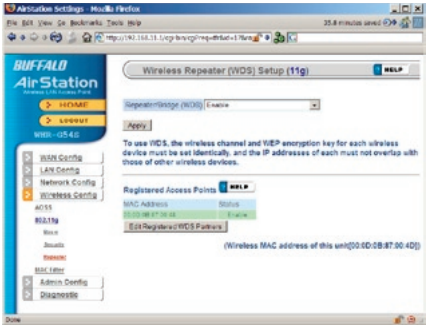
On the left side menu, click on *Wireless Config*, and then *Basic*.

Change the *Wireless Channel* from *Auto* to a channel. Make a note of the channel that you've chosen, because all of your wireless devices will need to be configured to use this same channel. Change *Frameburstring* from *125 High Speed Mode* to *Frameburstring* or *Do not use* (*Frameburstring* is recommended if all your client devices support it). Click *Apply*. Your AirStation will reboot in 30-60 seconds. Optional: Note the *SSID* of this AirStation. By default, this value will be different for each AirStation. For easy roaming, you may want to change the SSIDs of both AirStations to a constant value.

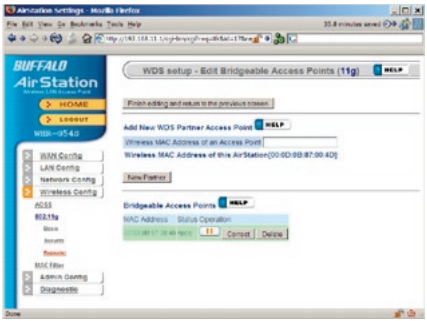


On the left-side menu, click on *Wireless Config*, and then *Repeater*.

Repeater-Bridge (WDS) must be set to *Enable*. If it is not, change it to *Enable* in the drop down menu and click *Apply*. After the AirStation reboots, the screen will refresh. Click *Edit Registered WDS Partners*.

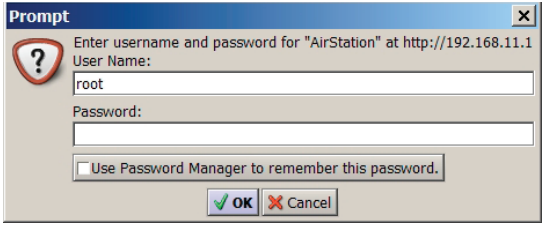


Under *Add New WDS Partner Access Point*, enter the wireless MAC address of the second AirStation, the one that you want to form a bridge with. You can get this from the bottom of the second AirStation (see above). Enter it with each pair of digits separated by a colon, e.g. 000D0B10F778 would be entered "00:0D:0B:10:F7:78". Press *New Partner* when done. The AirStation will reboot, and when the screen refreshes, the second AirStation's MAC address will be listed under *Bridgeable Access Points*.

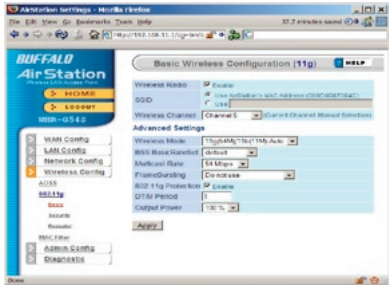


Now, you need to configure the second AirStation with the MAC address of the first one. In your browser's address field, enter "192.168.11.100". This will take you into the Web-Based Configuration Utility for the second AirStation.

Once again, the username is "root" and the password is blank by default.

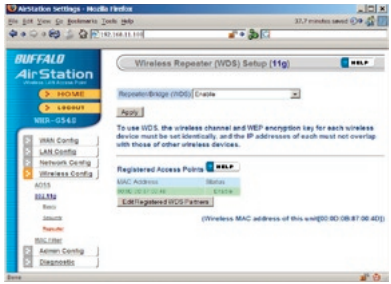


In the Web-Based Configuration Utility, click on the *Advanced* tab, select *Wireless Config*, and choose *Basic*. Change the wireless channel to match the one you set for the first AirStation. Change *Frameburstring* from *125 High Speed Mode* to *Frameburstring* or *Do not use* (whichever you chose for the first AirStation). For easy roaming, you may change the *SSID* to match the current SSID setting of the other AirStation. Click *Apply*. Your AirStation will reboot in 30-60 seconds.

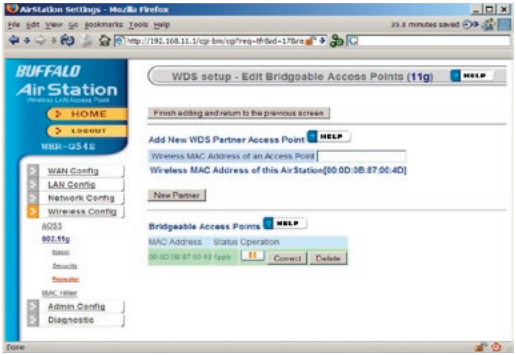


Now, under *Wireless Config*, choose *Repeater*.

Confirm that *Repeater-Bridge (WDS)* is set to *Enable*. Click *Edit Registered WDS Partners*.

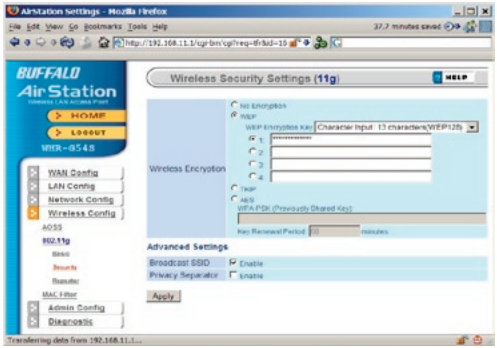


Under *Add New WDS Partner Access Point*, enter the wireless MAC address of the first AirStation (available from the bottom of the first AirStation), with each pair of digits separated by a colon, e.g. MAC:000D0B10F779 would be entered 00:0D:0B:10:F7:79. Click *New Partner* when done. The AirStation will reboot, and when the screen refreshes, the first AirStation's MAC address will be listed under *Bridgeable Access Points*.



The two AirStations are now linked by a wireless bridge. Unplug all the network cables and test the bridge by logging into each of the access points with a wireless client. You should be able to connect to either of the access points from Windows Wireless Network connection, getting an IP address assigned to your client with no error messages. You should also be able to log into both of their Web-Based Configuration Utilities by entering their IP addresses into a web browser (192.168.11.1 for the main access point; 192.168.11.100 for the bridged access point). If the first AirStation is connected to the Internet, you should be able to connect to the second AirStation and surf the web.

Once you can connect to each of your access points, you should configure WEP encryption. Without WEP, anyone within range of your access points can easily connect to your network. From within the second AirStation's Web-Based Configuration Utility (192.168.11.100), click on *Advanced*, then *Wireless Config*, then *Security*. Note that you must set up WEP on the bridge (second AirStation) first, before configuring it on the main router (first AirStation), or you will have to reconnect the network cables to finish configuration.



Change wireless encryption from "no encryption" to "WEP". Note that TKIP and AES encryption schemes will not work with WDS; you must use WEP for encryption. WEP keys may be any of 4 different types; choose one of the following types from the drop-down "WEP Encryption Key" box:

Character Input - 13 characters (ASCII WEP128 104 bit, key should contain 13 alphanumeric characters a-z, A-Z, 0-9)

Character Input - 5 characters (ASCII WEP64 40 bit, key should contain 5 alphanumeric characters a-z, A-Z, 0-9)

Hexadecimal Input - 26 digits (Hex WEP128 104 bit, key should contain 26 characters A-F, 0-9)

Hexadecimal Input - 10 digits (Hex WEP64 40 bit, key should contain 10 characters A-F, 0-9)

Enter at least one encryption key in the first encryption key space. The key should match the format of the chosen WEP encryption type. Additional keys may be entered in boxes 2, 3, and 4.

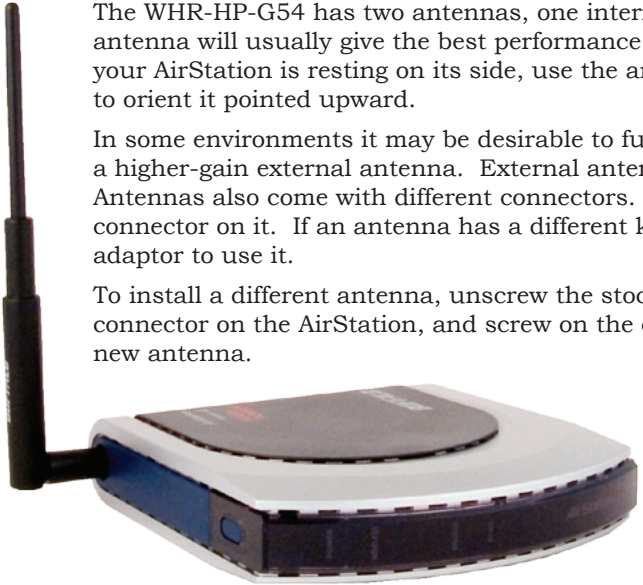
Click *Apply* when finished!

After configuring the bridge (the second AirStation) for WEP, log into the first AirStation's Web-Based Configuration Utility (192.168.11.1) and make exactly the same changes to the WEP settings. All WEP configuration settings must be exactly the same, or the AirStations will not be able to communicate.

Each wireless client that will connect to the AirStations must also be configured with the exact same WEP encryption key type and encryption key. Consult your wireless client's documentation for more information on configuring its WEP settings.

Once everything is working smoothly, change the admin password of both AirStations to something different from the default blank password. Store the new password in a safe place! You will not be able to access your network settings without it.

- Most problems with setting up WDS are caused by incorrectly entering the MAC addresses into each AirStation's Web-Based Configuration Utility. If you're having problems, check the MAC address settings in both AirStations's Web-Based Configuration Utilities. Each AirStation should be configured to be in a bridge with the other's wireless MAC address.
- Confirm that all bridges are set to the same wireless channel.
- If you cannot access the AirStations wirelessly, reconnect the Ethernet cables as shown on page 25 to easily access the AirStations's Web-Based Configuration Utilities.
- All wireless access points in the wireless bridge need to support WDS.
- No single access point can communicate with more then five other access points via wireless bridges.
- Start the wireless bridge system with only two access points and then add more, one at a time.
- Set up all access points in the wireless bridge in close proximity before deploying them to their final locations.
- Only one access point in the wireless bridge should be serving DHCP and routing services. If a wireless network is added to an existing routed wired network, none of the wireless devices should be serving DHCP.



The WHR-HP-G54 has two antennas, one internal and one external. The external antenna will usually give the best performance if oriented to point straight up. If your AirStation is resting on its side, use the antenna's swivel and twist function to orient it pointed upward.

In some environments it may be desirable to further increase range by installing a higher-gain external antenna. External antennas come in all shapes and sizes. Antennas also come with different connectors. The WHR-HP-G54 has an *RP-SMA* connector on it. If an antenna has a different kind of connector, you'll need an adaptor to use it.

To install a different antenna, unscrew the stock antenna from the RP-SMA connector on the AirStation, and screw on the connector or adaptor from your new antenna.

For more information, FAQs, and updates, consult the Buffalo Technology website at **www.buffalotech.com**.

WHR-HP-G54 AirStation Specifications

Physical Specifications

Dimensions 1.1 x 5.1 x 5.7 in. (28 x 130 x 144mm)
Weight 9.8 oz. lb. (277g)

Temperature & Humidity

Operation 0˚ to 40˚ C
Maximum humidity 80%
Transit/Storage 0˚ to 40˚ C maximum humidity 80% (no condensation)

Power Characteristics

Transmit Mode 1.1A (Nominal),
Power Supply 5 V output; 100-240V AC Universal, 50/60 Hz
Power Consumption about 6.5 Watts (Max)

Regulatory Information

Wireless communication is often subject to local radio regulations. Although AirStation wireless networking products have been designed for operation in the license-free 2.4 GHz band, local radio regulations may impose limitations on the use of wireless communication equipment.

Network Compatibility

IEEE802.11g/b Standard for Wireless LANs (125* High Speed Mode also Available.)

Host Operating System

Microsoft Windows® 98SE/ME/NT4.0/2000/XP, Unix, Linux and MacOS
Media Access Protocol
Wired - CSMD/CD (Collision Detection)
Wireless - CSMD/CA (Collision Avoidance) with Acknowledgment (ACK)

Radio Characteristics

RF Frequency Band 2.4 GHz (2400-2483 MHz)
11 selectable channels (3 non-overlapping)

Modulation Technique Direct Sequence Spread Spectrum

- ODFM for High Transmit Rate
- DQPSK for Standard Transmit Rate
- DBPSK for Low Transmit Rate

Spreading 11-chip Barker Sequence

Nominal Output Power: 19dBm (802.11b), 16dBm (802.11g)

Transmit Rate:

- High Speed 54 Mbps (125 Mbps in 125* High Speed Mode)
- Medium Speed 36 Mbps (96 Mbps in 125* High Speed Mode)
- Standard Speed 2 Mbps
- Low Speed 1 Mbps

Open Office Environment
160 m (525 ft.)
270 m (885 ft.)
400 m (1300 ft.)
550 m (1750 ft.)

Semi-Open Office Environment
50 m (165 ft.)
70 m (230 ft.)
90 m (300 ft.)
115 m (375 ft.)

Closed Office
25 m (80 ft.)
35 m (115 ft.)
40 m (130 ft.)
50 m (165 ft.)

Receiver Sensitivity -83 dBm -87 dBm -91 dBm -94 dBm (depends on data rate)

Delay Spread (at FER of <1%) 65 ns 225 ns 400 ns 500 ns (depends on data rate)

- The range of wireless devices can be affected by metal surfaces, solid high-density materials and obstacles in the signal path.

Table “Radio Characteristics” lists the typical ranges when used indoors:

- In Open Office environments, clients can “see” each other, i.e. there are no physical obstructions between them.
- In Semi-open Office environments, work space is separated by room dividers; client cards are at desktop level.
- In Closed Office environments, workspace is separated by floor-to-ceiling brick walls.

Note: The range values listed in Table “Radio Characteristics” are typical distances as measured at Buffalo Technology AirStation laboratories. These values are provided for your guidance but may vary according to the actual radio conditions at the location where the AirStation product is installed.

AirStation IEEE 802.11 Channel Sets

The range of the wireless signal is related to the Transmit Rate of the wireless communication. Communications at a lower Transmit range may travel longer distances.

Center Channel ID FCC

1 2412 2 2417 3 2422 4 2427 5 2432 6 2437 7 2442 8 2447 9 2452 10 2457
11 2462 11 default channel

Common Problems

- Out of range, client cannot connect to the AirStation.
- Configuration mismatch, client cannot connect to the AirStation.
- Absence or conflict with the Client Driver.
- Conflict of another device with the AirStation hardware.

LED Activity

Monitoring LED activity may help identify problems.

- Power LED should be Green when the AirStation is on.
- The Security LED lights when encryption or authorization is turned on.
- Wireless LED should be Green if the line is active. If it is blinking Green, wireless communication is active.
- Router LED should be Green (100Mbps) or Amber (10Mbps) while communication is active.
- The Red Diag LED will flash during boot and firmware updates. 3 red flashes at boot indicates a problem with the wired LAN side. 4 red flashes at boot indicates a problem with the wireless LAN side.

To check the Diag LED, unplug the power for three seconds. Plug the power back in and watch the Diag LED during boot-up.

LEDs Work But Client PC Cannot Connect to Network

If the LEDs indicate that the network is working properly (Power LED is on, Transmit/Receive LED blinks), check the TCP/IP settings of the network.

Changing Client TCP/IP Settings in Windows

Consult the LAN Administrator for correct TCP/IP settings.

To add or change TCP/IP Settings:

1. On the Windows task bar, click Start.
2. Select Settings, then Control Panel.
3. Double-click on the Network icon to view Network Properties.
4. From the list of installed components, verify the "TCP/IP - wireless LAN adapter" protocol is installed.
   - If the wireless adapter protocol is not yet installed, click the *Add* button and select the TCP/IP protocol from the list. Refer to Windows Help for more information.
   - If the wireless adapter protocol is installed, select the protocol and click the *Properties* button. Verify that the parameters match the settings provided by your LAN Administrator. Make changes if necessary, and click OK.
5. If prompted, restart your computer.

Other Problems

Please refer to **www.buffalotech.com** for further reference materials.

10BaseT: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 10 Mbps data transmission speed.

100BaseT: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 100 Mbps data transmission speed.

1000BaseT: 802.3 based Ethernet network that uses UTP (Unshielded twisted pair) cable and a star topology. 1000 Mbps data transmission speed.

802.1x: The standard for wireless LAN authentication used between an AP and a client. 802.1x with EAP will initiate key handling.

Access Point: A hardware device that acts as a communication hub for *Clients* (users of wireless devices) to connect to a wired LAN.

Bandwidth: The transmission capacity of a computer or a communication channel, usually stated in Megabits per second (Mbps).

Bridge: A device which forwards traffic between network segments with a common network layer address, based on data link layer information.

Client: A PC, workstation, or other device that connects to a network wirelessly through an *Access Point*.

Cross-Over Cable: A UTP cable that has its transmit and receive pair crossed to allow communications between two devices.

Default Gateway: The IP Address of either the nearest router or server for the LAN.

Destination Address: The address portion of a packet that identifies the intended recipient station.

DHCP (Dynamic Host Configuration Protocol): Based on BOOTP, it uses a pool of IP addresses, which it assigns to each device connected to it, and retrieves the address when the device becomes dormant for a period of time.

DNS (Domain Name System): System used to map readable machine names into IP addresses.

Driver: Software that interfaces a computer with a specific hardware device.

Dynamic IP Address: An IP address that is automatically assigned to a client station in a TCP/IP network, typically by a DHCP server.

Ethernet: The most widely used architecture for Local Area Networks (LANs). It is a shared-media network architecture. The IEEE 802.3 standard details its functionality.

Ethernet cable: A wire similar to telephone cable that carries signals between Ethernet devices. It is designed to connect a single device's NIC to a router, switch, or hub. See also *Crossover cable*.

File and Print Sharing: A Microsoft application that allows computers on a network to share files and printers.

Firmware: Computer programming instructions that are stored in a read-only memory unit rather than being implemented through software.

Frame: A fixed block of data, transmitted as a single entity. Also referred to as a packet.

Full-Duplex: To transmit in both directions simultaneously.

Half-duplex: To transmit in both directions, one direction at a time.

Hub: A device which allows connection of computers and other devices to form a LAN.

IEEE (Institute of Electrical and Electronics Engineers): The professional organization which promotes development of electronics technology.

IP (Internet Protocol) Address: A unique 32-binary-digit number that identifies each sender or receiver of information sent in packets.

Infrastructure: A wireless network or other small network in which the wireless network devices are made a part of the network through the Access Point.

ISP (Internet Service Provider): A company that provides access to the Internet and other related services.

IV (Initialization Vector): The header section of an encrypted message packet.

LAN (Local Area Network): A group of computers and peripheral devices connected to share resources.

LED (Light Emitting Diode): The lights on a hardware device representing the activity through the ports.

MAC (Medium Access Control) Address: The unique number that distinguishes every network interface card.

Mbps (Mega Bits Per Second): A measurement of millions of bits per second.

MDI/X (Media Dependent Interface/ Cross-over): Port on a network hub or switch that crosses the incoming transmit lines with the outgoing receive lines.

MHz (MegaHertz): One million cycles per second.

NAT (Network Address Translation): An internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set for external traffic.

NIC (Network Interface Card): An expansion card connected to a computer so the computer can be connected to a network.

Packet: A block of data that is transferred as a single unit, also called a frame or a block.

Packet Filtering: Discarding unwanted network traffic based on its originating address or its type.

PCMCIA (Personal Computer Memory Card International Association) Card: Removable module that adds features to a portable computer.

Ping (Packet Internet Groper): An Internet utility used to determine whether a particular IP address is accessible.

Plug and Play: Hardware that, once physically installed, finishes its installation automatically and may immediately be used, as opposed to hardware that requires further manual configuration.

PoE (Power over Ethernet): A mechanism to send DC power to a device along its Ethernet cable.

PPPoE (Point-to-Point Protocol over Ethernet): A specification for connecting users on an Ethernet line to the Internet through a common broadband medium.

Protocol: A standard way of exchanging information between computers.

RADIUS (Remote Authentication Dial In User Service): A server that issues authentication keys to clients.

RAM (Random Access Memory): Non-permanent memory.

RJ-45 connector: An 8-pin connector used between a twisted pair cable and a data transmission device.

ROM (Read Only Memory): Memory hardware that allows fast access to permanently stored data but prevents addition to or modification of the data.

Roaming: The ability to use a wireless device while moving from one access point to another without losing the connection.

SMTP (Simple Mail Transfer Protocol): The protocol used to define and deliver electronic mail (E-mail) from one location to another.

SNMP (Simple Network Management Protocol): An application layer protocol that outlines the formal structure for communication among network devices.

Static IP Address: A permanent IP address assigned to a node in a TCP/IP network.

SSID: The "name" of your wireless network. You can get it from the Setup page of the configuration utility.

STP (Shielded Twisted Pair): Twisted Pair cable wrapped in a metal sheath to provide extra protection from external interfering signals.

Subnet Mask: An eight-byte address divided into 4 parts separated by periods.

TCP/IP (Transmission Control Protocol/ Internet Protocol: Protocol used by computers when communicating across the Internet or Intranet.

TKIP (Temporal Key Integrity Protocol): An encryption method replacing WEP. TKIP uses random IV and frequent key exchanges.

Twisted Pair: Cable that comprises 2 or more pair of insulated wires twisted together.

UDP (User Datagram Protocol): A communication method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network. UDP is used as an alternative to TCP/IP.

UTP (Unshielded Twisted Pair) cable: Two or more unshielded wires twisted together to form a cable.

WAN (Wide Area Network): A networking system covering a wide geographical area.

WEP Encryption: A common security protocol for wireless networks. WEP is compatible with almost all wireless devices.

Web Browser: A software program that allows viewing of web pages.

Wi-Fi (Wireless Fidelity): An organization that tests and assures interoperability among WLAN devices.

WLAN (Wireless LAN): A LAN topology using wireless devices.

WPA Encryption: An encryption algorithm designed to improve on the security of WEP.

WPA2 Encryption: An advanced AES-based encryption algorithm. This is the latest, best security algorithm currently available for Buffalo Wi-Fi products.

VPN (Virtual Private Network): A security method to connect remote LAN users to a corporate LAN system.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Warning:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Important Note - FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for uncontrolled equipment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Important Note - Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

European Union Notice:

Radio products with the CE marking comply with the R&TTE Directive (1999/5/EC), the EMC Directive (89/336/EEC) and the Low Voltage Directive (73/23/EEC) issued by the Commission of the European Community.
Compliance with these directives implies conformity to the following European Norms:

- EN 60950 Product Safety
- EN 300 328 Technical requirement for radio equipment
- EN 301 489-1/-17 General EMC requirements for radio equipment

Taiwan:

SAR compliance has been established in typical laptop computer(s) with CardBus slot, and product could be used in typical laptop computer with CardBus slot. Other application like handheld PC or similar device has not been verified, may not comply with related RF exposure rules, and such use shall be prohibited.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of

the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

Intended use

This device is a 2.4 GHz wireless LAN transceiver, intended for indoor home and office use in USA, Canada, all EU and EFTA member states.

EU Countries intended for use

This device is intended for indoor home and office use in the following countries: Austria, Belgium, Denmark, France, Finland, Germany, Greece, Italy, Ireland, Luxembourg, The Netherlands, Portugal, Spain, Sweden, United Kingdom, Cyprus, Czech Republic, Estonia, Hungry, Latvia, Lithuania, Malta, Poland, Slovak Republic, and Slovenia.

The device is also authorized for use in all EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU countries not intended for use

None

Potential restrictive use

This device is a 2.4 GHz wireless LAN transceiver, intended for indoor home and office use in all EU and EFTA member states, except in France, Belgium and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain an authorization to use the device for setting up outdoor radio links.

In Belgium there is a restriction in outdoor use. The frequency range in which outdoor operation in Belgium is permitted is 2460 – 2483.5 MHz.

In France only channels 10,11,12 and 13 are available.

This device may not be used for setting up outdoor radio links in France. For more information see **http://www.anfr.fr/** and/or **http://www.art-telecom.fr**

- The equipment that you have purchased has required the extraction and use of natural resources for its production.
- The equipment may contain hazardous substances that could impact health and the environment.
- In order to avoid the dissemination of those substances in our environment and to diminish the pressure on the natural resources, we encourage you to use the appropriate take-back systems.
- The take-back systems will reuse or recycle most of the materials of your end life equipment in a sound way.
- The crossed-out wheeled bin symbol invites you to use those systems.

- If you need more information on the collection, reuse and recycling systems, please contact your local or regional waste administration.

Buffalo Technology (Melco Inc.) products come with a two-year limited warranty from the date of purchase. Buffalo Technology (Melco Inc.) warrants to the original purchaser the product; good operating condition for the warranty period. This warranty does not include non-Buffalo Technology (Melco Inc.) installed components. If the Buffalo product malfunctions during the warranty period, Buffalo Technology/(Melco Inc.) will replace the unit, provided the unit has not been subjected to misuse, abuse, or non-Buffalo Technology/(Melco Inc.) authorized alteration, modifications or repair.

All expressed and implied warranties for the Buffalo Technology (Melco Inc) product line including, but not limited to, the warranties of merchantability and fitness of a particular purpose are limited in duration to the above period.

Under no circumstances shall Buffalo Technology/(Melco Inc.) be liable in any way to the user for damages, including any lost profits, lost savings or other incidental or consequential damages arising out of the use of, or inability to use the Buffalo products.

In no event shall Buffalo Technology/(Melco Inc.) liability exceed the price paid for the product from direct, indirect, special, incidental, or consequential damages resulting from the use of the product, its accompanying software, or its documentation. Buffalo Technology/(Melco Inc.) does not offer refunds for any product.

Buffalo Technology USA Inc.
11100 Metric Blvd, Suite 750
Austin, TX 78758

GENERAL INQUIRIES

Monday through Friday
8:30am-5:30pm CST
Direct: 512-794-8533 | **Toll-free:** 800-456-9799 | **Fax:** 512-794-8520 | **Email:** *sales@buffalotech.com*

TECHNICAL SUPPORT

North American Technical Support by phone is available 24 hours a day, 7 days a week. (USA and Canada).
Toll-free: (866) 752-6210 | **Email:** *info@buffalotech.com*

Buffalo Technology UK Ltd.
2 Bracknell Beeches, Old Bracknell Lane
Bracknell, Berkshire, RG12 7BW
United Kingdom

GENERAL INQUIRIES

Email: *sales@buffalo-technology.com*

TECHNICAL SUPPORT

Buffalo Technology provides technical support in English, German, French, Italian, and Spanish. For opening hours and relevant telephone numbers, please go to

www.buffalo-technology.com/contact

Source code for Buffalo products that use GPL code is available at *http://opensource.buffalo.jp*.

* When operating in High-Speed Mode, this Wi-Fi device achieves an actual throughput of up to 34.1 Mbps, which is equivalent to the throughput of a system following 802.11g protocol and operating at a signaling rate of 125 Mbps.